

18.09.00

JP 00/5439

日本国特許庁

PATENT OFFICE
JAPANESE GOVERNMENT

22/2

別紙添付の書類に記載されている事項は下記の出願書類に記載されて
いる事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed
with this Office.

出願年月日

Date of Application:

1999年 8月12日

REC'D 03 OCT 2000

WIPO

PCT

出願番号

Application Number:

平成11年特許願第228154号

出願人

Applicant(s):

松下電器産業株式会社

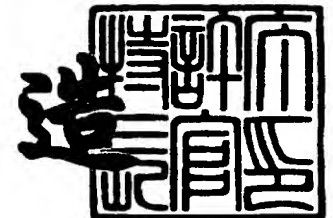
09/807295

PRIORITY
DOCUMENTSUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH RULE 17.1(a) OR (b)

2000年 8月25日

特許庁長官
Commissioner,
Patent Office

及川耕造



出証番号 出証特2000-3068162

出 願 人 履 歴 情 報

識別番号

[000005821]

1. 変更年月日 1990年 8月28日

[変更理由] 新規登録

住 所 大阪府門真市大字門真1006番地

氏 名 松下電器産業株式会社

【書類名】 特許願
 【整理番号】 2030714021
 【提出日】 平成11年 8月12日

【あて先】 特許庁長官殿

【国際特許分類】 H04M 15/00

【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地
 松下電器産業株式会社内

【氏名】 中西 良明

【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地
 松下電器産業株式会社内

【氏名】 高山 久

【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地
 松下電器産業株式会社内

【氏名】 松瀬 哲朗

【特許出願人】

【識別番号】 000005821

【氏名又は名称】 松下電器産業株式会社

【代理人】

【識別番号】 100082692

【弁理士】

【氏名又は名称】 蔵合 正博

【電話番号】 03(3519)2611

【手数料の表示】

【予納台帳番号】 013549

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9004843

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 電子価値情報バックアップシステム及びこれに用いる装置

【特許請求の範囲】

【請求項 1】 電子現金・電子チケット等の電子価値情報を管理する電子財布手段と、前記電子財布手段が管理する電子価値情報を保持する電子財布記憶手段と、前記電子財布手段が管理する電子価値情報を通信によって登録することを受け付けその登録証を発行する電子金庫手段と前記電子価値情報を保管する電子金庫保管手段を持ち、前記電子財布手段は前記電子金庫手段に対して前記登録証を提示することで前記電子金庫保管手段に登録された前記電子価値情報を取り出すことが出来ることを特徴とする電子価値情報バックアップシステム。

【請求項 2】 登録証に電子価値情報の部分情報が含まれることを特徴とする請求項 1 記載の電子価値情報バックアップシステム。

【請求項 3】 電子財布手段固有の暗号鍵と復号鍵を保持する鍵保管手段と、前記暗号鍵を用いた暗号化および前記復号鍵を用いた復号化を行なう暗号化手段を追加し、電子価値情報を前記暗号化手段によって暗号化したものを電子金庫手段へ登録することを特徴とする請求項 1 記載の電子価値情報バックアップシステム。

【請求項 4】 請求項 3 に鍵管理手段と前記鍵管理手段の記憶領域である鍵管理記憶手段を追加し、前記鍵管理手段に前記鍵保管手段に保持された復号鍵を暗号化手段が登録することによって、前記鍵保管手段の破損や紛失などの原因によって前記復号鍵が消失した時に前記暗号化手段が前記鍵管理手段から前記復号鍵を復元することを可能とすることを特徴とする請求項 3 記載の電子価値情報バックアップシステム。

【請求項 5】 請求項 3 の鍵保管手段上に請求項 3 の暗号化手段が暗号鍵と復号鍵のペアを生成することを特徴とする請求項 3 記載の電子価値情報バックアップシステム。

【請求項 6】 鍵管理手段が暗号鍵と復号鍵のペアを生成し、鍵保管手段に前記鍵ペアを配布することを特徴とする請求項 4 記載の電子価値情報バックアップシステム。

【請求項 7】 鍵管理手段に復号鍵を 2 つに分割した一方の部分鍵を登録し、他方の部分鍵を暗号化された電子価値情報と組として電子金庫手段に登録することを特徴とする請求項 4 記載の電子価値情報バックアップシステム。

【請求項 8】 請求項 7 での部分鍵として、暗号鍵と復号鍵を数学的に生成するための元となった情報を 2 つに分割して一方を鍵管理手段に登録する部分鍵、他方を電子金庫手段に登録する部分鍵とすることを特徴とする請求項 7 記載の電子価値情報バックアップシステム。

【請求項 9】 電子財布手段から電子金庫手段に電子価値情報を登録し、前記電子金庫手段から送られた登録証に対する検証が成功した場合、登録済みの前記電子価値情報を電子財布手段から削除して対応する登録証のみを保管することを特徴とする請求項 1 記載の電子価値情報バックアップシステム。

【請求項 10】 暗号化手段が扱う暗号化方式を共通鍵方式として、暗号鍵と復号鍵に同じ鍵を用いることを特徴とする請求項 3 記載の電子価値情報バックアップシステム。

【請求項 11】 暗号化手段が扱う暗号化方式を公開鍵方式として、暗号鍵と復号鍵を非対称鍵とすることを特徴とする請求項 3 記載の電子価値情報バックアップシステム。

【請求項 12】 鍵保管手段の所有者固有の情報を鍵管理手段に復号鍵と関連付けて所有者認証情報として登録することと、前記所有者固有の情報を鍵管理手段に提示して認証が成功した場合に前記復号鍵を前記鍵保管手段に復元することを特徴とする請求項 4 記載の電子価値情報バックアップシステム。

【請求項 13】 所有者認証情報として鍵保管手段とは独立した IC カードに蓄積されたカード所有者を特定するための情報を用いることを特徴とする請求項 12 記載の電子価値情報バックアップシステム。

【請求項 14】 所有者認証情報として所有者の生体特徴情報を用いることを特徴とする請求項 12 記載の電子価値情報バックアップシステム。

【請求項 15】 鍵管理手段に対する所有者の正当性認証が成功した場合に、前記鍵管理手段が電子金庫手段と通信を行ない暗号化された電子価値情報を取得し、前記暗号化された電子価値情報の復号化を行なった電子価値情報を前記電子

財布記憶手段上に復元することを特徴とする請求項 12 記載の電子価値情報バックアップ装置。

【請求項 16】 鍵管理手段に対して所有者の正当性認証が成功した場合に、前記鍵管理手段が電子金庫手段と通信を行ない暗号化された電子価値情報を取得し、前記暗号化された電子価値情報の復号化を行なった電子価値情報を新しく生成した暗号鍵を用いて暗号化し、前記の新しい暗号鍵で暗号化された前記電子価値情報を電子金庫上の古い暗号鍵で暗号化された前記電子価値情報と置き換え、前記鍵管理手段が新しい暗号鍵と復号鍵を鍵保管手段に配布することを特徴とする請求項 12 記載の電子価値情報バックアップシステム。

【請求項 17】 鍵管理手段に対して所有者の正当性認証が成功した場合に、前記鍵管理手段が電子金庫手段と通信を行ない暗号化された電子価値情報を取得し、前記暗号化された電子価値情報の復号化を行なった電子価値情報を新しく生成した暗号鍵を用いて暗号化し、前記の新しい暗号鍵で暗号化された前記電子価値情報を電子財布手段上に復元し、前記鍵管理手段が新しい暗号鍵と復号鍵を鍵保管手段に配布することを特徴とする請求項 12 記載の電子価値情報バックアップシステム。

【請求項 18】 電子財布手段が保管する電子価値情報に対して前記電子財布手段上のバックアップ条件情報と照合を行ない、条件に合致する電子価値情報を自動的に電子金庫手段に登録し登録証を受けとることを特徴とする請求項 1 記載の電子価値情報バックアップシステム。

【請求項 19】 バックアップ条件情報をユーザが変更できるようにすることを特徴とする請求項 18 記載の電子価値情報バックアップシステム。

【請求項 20】 バックアップ条件情報として、電子価値情報の種類を用いることを特徴とする請求項 18 記載の電子価値情報バックアップシステム。

【請求項 21】 バックアップ条件情報として、電子価値情報のサイズを用いることを特徴とする請求項 18 記載の電子価値情報バックアップシステム。

【請求項 22】 バックアップ条件情報として、電子価値情報のサイズと電子財布記憶手段の空きメモリ容量を用いることを特徴とする請求項 18 記載の電子価値情報バックアップシステム。

【請求項 23】 バックアップ条件情報として、電子価値情報の有効期限を用いることを特徴とする請求項 18 記載の電子価値情報バックアップシステム。

【請求項 24】 バックアップ条件情報として、電子価値情報の保持開始時間を用いることを特徴とする請求項 18 記載の電子価値情報バックアップシステム

【請求項 25】 電子財布手段が登録証を提示して前記電子価値情報を前記電子財布手段上に復元する時、復元に十分な容量が電子財布上に残っていない場合、容量不足をユーザに対して提示し復元作業を中断することを特徴とする請求項 1 記載の電子価値情報バックアップシステム。

【請求項 26】 電子財布手段が登録証を提示して前記電子価値情報を前記電子財布手段上に復元する時または新規の電子価値情報を登録する時、復元や新規登録に十分な容量が電子財布記憶手段上に残っていない場合、電子財布手段上のバックアップ条件情報に基づいて現在保持されている電子価値情報を自動的に電子金庫手段に登録し登録証と置き換え、電子金庫上の電子価値情報を復元するための領域を空けることによって復元作業を継続することを特徴とする請求項 1 記載の電子価値情報バックアップシステム。

【請求項 27】 電子財布手段が電子価値情報の登録証を提示して前記電子価値情報を前記電子財布手段上に復元する時または新規の電子価値情報を登録する時、復元や新規登録に十分な容量が電子財布記憶手段上に残っていない場合、処理の中断および処理継続の方法を提示して選択させることで、復元作業の中断もしくはは継続することを特徴とする請求項 26 記載の電子価値情報バックアップシステム。

【請求項 28】 電子価値情報と登録証を保管する電子財布記憶手段を備え、電子金庫手段に対して通信を行うことを特徴とする電子財布手段。

【請求項 29】 登録証に電子価値情報の部分情報を含む事を特徴とする請求項 28 記載の電子財布手段。

【請求項 30】 電子価値情報と登録証を保管する電子財布記憶手段と、電子価値情報を暗号化する暗号鍵と、暗号化された電子情報を復号化する復号鍵とを有する暗号化手段を備え、電子金庫手段に対して通信を行うことを特徴とする電

子財布手段。

【請求項 31】 請求項 30 の復号鍵を 2 つに分割した部分鍵の一方を電子価値情報と組にして電子金庫手段に登録することを特徴とする請求項 30 記載の電子財布手段。

【請求項 32】 請求項 31 の部分鍵を、暗号鍵と復号鍵を数学的に生成する元となった情報を 2 つに分割した一方とすることを特徴とする請求項 31 記載の電子財布手段。

【請求項 33】 前記電子金庫手段から送られた登録証が、バックアップする電子価値情報に対応する登録証であることを検証する登録証検証手段を備え、前記電子金庫手段から登録証を取得した際、前記登録証が前記バックアップする電子価値情報に対応する登録証であることが検証された場合に、前記登録証に対応する電子価値情報を電子財布記憶手段上から削除することを特徴とする請求項 28 記載の電子財布手段。

【請求項 34】 設定されたバックアップ条件情報との照合を行ない、条件に合致する電子価値情報を自動的に電子金庫手段に登録して登録証を取得することを特徴とする請求項 28 記載の電子財布手段。

【請求項 35】 電子価値情報の復元時または新規登録時に電子財布記憶手段上に十分な記憶容量が残っていない場合、容量不足をユーザに対して提示し復元作業を中断することを特徴とする請求項 28 記載の電子財布手段。

【請求項 36】 電子価値情報の復元時または新規登録時に電子財布記憶手段上に十分な記憶容量が残っていない場合、自動的にバックアップ条件情報に基づいて電子価値情報のバックアップを行って記憶容量を確保することを特徴とする請求項 28 記載の電子財布手段。

【請求項 37】 電子価値情報の復元時または新規登録時に電子財布記憶手段上に十分な記憶容量が残っていない場合、容量不足を提示して復元作業を中断するか自動的にバックアップ条件情報に基づいてバックアップを行なって記憶容量を確保するかをユーザに選択させることを特徴とする請求項 28 記載の電子財布手段。

【請求項 38】 電子価値情報を保管する電子金庫記憶手段を備え、電子価値

情報から登録証を生成することと、登録証に対応する電子価値情報を電子金庫記憶手段から引き出すことを特徴とする電子金庫手段。

【請求項 3 9】 登録証に電子価値情報の部分情報が含まれる事を特徴とする請求項 3 8 記載の電子金庫手段。

【請求項 4 0】 暗号化された電子価値情報の登録を受けて登録証を生成し、登録証の提示を受けて暗号化された電子価値情報を返すことを特徴とする請求項 3 8 記載の電子金庫手段。

【請求項 4 1】 復号鍵を 2 つに分割した一方の部分鍵と暗号化した電子価値情報の登録を受けて登録証を生成し、登録証の提示を受けて暗号化された電子価値情報と部分鍵を返す事を特徴とする請求項 4 0 記載の電子金庫手段。

【請求項 4 2】 請求項 4 1 の部分鍵を、暗号鍵と復号鍵を数学的に生成する元となった情報を 2 つに分割した一方とすることを特徴とする請求項 4 1 記載の電子金庫手段。

【請求項 4 3】 登録要求を受けた鍵を保管する鍵管理記憶手段を備える事を特徴とする鍵管理手段。

【請求項 4 4】 登録要求を受けた鍵を認証情報と組にして保管する鍵管理記憶手段を備え、認証情報が一致する場合のみ前記鍵管理記憶手段上に登録された鍵を引き出す事を可能とする事を特徴とする鍵管理手段。

【請求項 4 5】 暗号鍵と復号鍵の鍵ペアを生成して鍵管理記憶手段上に保管するとともに暗号化手段に対して配布する事を特徴とする鍵管理手段。

【請求項 4 6】 電子金庫手段と通信して、電子金庫手段上の暗号化された電子価値情報を鍵管理記憶手段上の復号鍵を用いて復号し、新しく暗号鍵と復号鍵の鍵ペアを生成し、新しい暗号鍵を用いて前記電子価値情報を暗号化した電子価値情報を古い暗号化された電子価値情報との置き換えることを電子金庫手段に対して要求し、新しい鍵ペアを暗号化手段に配布することを特徴とする鍵管理手段。

【請求項 4 7】 電子金庫手段と通信して、電子金庫手段上の暗号化された電子価値情報を鍵管理記憶手段上の復号鍵を用いて復号し、前記電子価値情報を電子財布手段に送ることを特徴とする鍵管理手段。

【請求項 48】 鍵管理手段と通信して所有者認証に基づいて復号鍵の登録と取得を行なうことを特徴とする暗号化手段。

【請求項 49】 電子金庫手段と通信して登録証と対応する一方の分割鍵を取得し、鍵管理手段と通信して所有者認証に基づいて他方の分割鍵を取得し、2つの分割鍵を用いて復号鍵を復元することを特徴とする暗号化手段。

【請求項 50】 請求項 1 から請求項 27 および請求項 28 から請求項 37 に記載の電子財布手段の制御プログラムを、電子計算機が読み取り可能な形式で記録した制御プログラム記録媒体。

【請求項 51】 請求項 1 から請求項 27 および請求項 37 から請求項 42 に記載の電子金庫手段の制御プログラムを、電子計算機が読み取り可能な形式で記録した制御プログラム記録媒体。

【請求項 52】 請求項 3 から請求項 27 および請求項 43 から請求項 47 に記載の鍵管理手段の制御プログラムを、電子計算機が読み取り可能な形式で記録した制御プログラム記録媒体。

【請求項 53】 請求項 2 から請求項 27 および請求項 48 から請求項 49 に記載の暗号化手段の制御プログラムを、電子計算機が読み取り可能な形式で記録した制御プログラム記憶媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明はコンピュータと情報通信を用いたバックアップシステム、特に電子マネーや電子チケットといった電子価値情報のバックアップと復元を行なう電子価値情報システムに関するものである。

【0002】

【従来の技術】

電子現金や電子チケットなどの金銭もしくは金銭的価値のある情報を、電子的な形式で表現し利用する技術が一般的となってきた。電子現金や電子チケットなどの電子的に表現された価値情報を、以下、電子価値情報とする。

【0003】

電子価値情報の実現方法の一つとして、遠隔地のサーバ上で電子価値情報を置き、その所有者は認証情報のみを持ち、利用時にサーバと通信するようにする方法がある。前記の方法では、認証の安全性を確保する事によって安全な取り引きを実現できるが、ネットワークに接続できる状態でなければ電子価値情報を使用できないという問題や、ネットワークへの問い合わせが使用の度に発生するため、高速な反応を要求する状況には適用しにくいという問題がある。

【0004】

そのため、ネットワークと独立した状態でも電子価値情報を利用することが出来るように、電子価値所有者の持つICカード、携帯電話、携帯端末などのデバイス上に電子価値情報そのものを保持するようにする技術も存在する。ただしこの場合、デバイスの破損や紛失によって電子価値情報が消失してしまう危険性を持っている。

【0005】

上記の電子価値情報を含む電子情報の破壊という問題からの回復を実現するため、従来いくつかの技術が考案されている。以下にその例を示す。

【0006】

第一の従来技術として、特開平10-133925号公報に示される技術では、暗号化したメールを用いることで、ファイヤーウォール内から外のバックアップサーバに対してデータのバックアップを行う。ただしこの技術では、鍵の紛失や破損時に暗号化したデータからの復元方法についてを考慮していない。

【0007】

第二の従来技術として、米国特許5, 778, 395に示される技術では、ネットワークに繋がったノード(コンピュータ)のファイルを別のノード上のサーバに圧縮や暗号化を行ってバックアップする。ただしこの技術でも、第一の従来技術と同様に鍵の紛失や破損時のことを考慮していない。

【0008】

【発明が解決しようとする課題】

しかしながら、上述の従来技術は、暗号によって秘置した状態で電子情報のバックアップと復元を行うものであった。しかし、従来技術では、暗号に用いた鍵

情報が消失した場合に暗号化されたバックアップ情報を復元することについて考慮されていないため、デバイスの破壊などに対処できないという問題がある。また、暗号の復号に用いる鍵をバックアップする場合、鍵のバックアップ管理の信頼性によらず、不正行為を排除しなければならない。

【0009】

本発明は、上記のような問題に鑑みてなされたもので、通信を介してサーバ上に電子価値情報を安全にバックアップすることと、バックアップと復元の際に不正行為が行われないうことと、鍵情報消失の緊急時の電子価値情報のバックアップからの復元を可能とする手段を提供することを目的とする。

【0010】

【課題を解決するための手段】

上記課題を解決するために、本発明は第1にローカルの電子価値情報を暗号化してサーバ上にバックアップする。これにより、電子価値情報をサーバに隠蔽した状態でバックアップすることと、ローカルの電子価値情報が破損した場合にも電子価値情報を復元することが可能になる。

【0011】

また、第2に暗号化した電子価値情報の復号鍵を電子価値情報のバックアップ先のサーバとは別のサーバにバックアップする。これにより、ローカルの復号鍵が破損した場合にも復号鍵を復元する事によって暗号化した電子価値情報を復元する事が可能になる。

【0012】

また、第3に復号鍵を分割してそれぞれを別々にバックアップする。これにより、復号鍵の全体を知られる事なく、ローカルに復号鍵を復元することが可能になる。

【0013】

また、第4に復号鍵をバックアップしたサーバに、暗号化した電子価値情報を復号させて電子価値情報をローカルに復元する。これにより、ローカルデバイスが壊滅的に破損または紛失した場合にも、電子価値情報を復元する事が可能になる。

【0014】

また、第5に復号鍵をバックアップしたサーバに、暗号化した電子価値情報を復号させ、新しい暗号化を行なわせて登録しなおし、新しい鍵情報をローカル環境に再配布させる。これにより、ローカル環境の鍵情報のみが破損または紛失した場合にも、ローカル環境に与える影響を小さく抑えた上でバックアップした電子価値情報を復元できる環境を再構築することが可能となる。

【0015】

このような各種態様を有する発明として、本発明の請求項1に記載の発明は、電子価値情報バックアップシステムとして、電子現金・電子チケット等の電子価値情報を管理する電子財布手段と、前記電子財布手段が管理する電子価値情報を保持する電子財布記憶手段と、前記電子財布手段が管理する電子価値情報を通信によって登録することを受け付けその登録証を発行する電子金庫手段と前記電子価値情報を保管する電子金庫保管手段を持ち、前記電子財布手段は前記電子金庫手段に対して前記登録証を提示することで前記電子金庫保管手段に登録された前記電子価値情報を取り出すことが出来るようにしたものである。

【0016】

本発明の請求項2に記載の発明は、請求項1に記載の電子価値情報バックアップシステムにおいて、登録証に電子価値情報の部分情報が含まれるようにしたものである。

【0017】

本発明の請求項3に記載の発明は、請求項1に記載の電子価値情報バックアップシステムにおいて、電子財布手段固有の暗号鍵と復号鍵を保持する鍵保管手段と、前記暗号鍵を用いた暗号化および前記復号鍵を用いた復号化を行なう暗号化手段を追加し、電子価値情報を前記暗号化手段によって暗号化したものを電子金庫手段へ登録するようにしたものである。

【0018】

本発明の請求項4に記載の発明は、請求項3に記載の電子価値情報バックアップシステムにおいて、請求項3に鍵管理手段と前記鍵管理手段の記憶領域である鍵管理記憶手段を追加し、前記鍵管理手段に前記鍵保管手段に保持された復号鍵を

暗号化手段が登録することによって、前記鍵保管手段の破損や紛失などの原因によって前記復号鍵が消失した時に前記暗号化手段が前記鍵管理手段から前記復号鍵を復元することを可能としたものである。

【 0 0 1 9 】

本発明の請求項 5 に記載の発明は、請求項 3 記載の電子価値情報バックアップシステムにおいて、請求項 3 の鍵保管手段上に請求項 3 の暗号化手段が暗号鍵と復号鍵のペアを生成するようにしたものである。

【 0 0 2 0 】

本発明の請求項 6 に記載の発明は、請求項 4 記載の電子価値情報バックアップシステムにおいて、鍵管理手段が暗号鍵と復号鍵のペアを生成し、鍵保管手段に前記鍵ペアを配布するようにしたものである。

【 0 0 2 1 】

本発明の請求項 7 に記載の発明は、請求項 4 記載の電子価値情報バックアップシステムにおいて、鍵管理手段に復号鍵を 2 つに分割した一方の部分鍵を登録し、他方の部分鍵を暗号化された電子価値情報と組として電子金庫手段に登録するようにしたものである。

【 0 0 2 2 】

本発明の請求項 8 に記載の発明は、請求項 7 記載の電子価値情報バックアップシステムにおいて、請求項 7 での部分鍵として、暗号鍵と復号鍵を数学的に生成するための元となった情報を 2 つに分割して一方を鍵管理手段に登録する部分鍵、他方を電子金庫手段に登録する部分鍵とするようにしたものである。

【 0 0 2 3 】

本発明の請求項 9 に記載の発明は、請求項 1 記載の電子価値情報バックアップシステムにおいて、電子財布手段から電子金庫手段に電子価値情報を登録し、前記電子金庫手段から送られた登録証に対する検証が成功した場合、登録済みの前記電子価値情報を電子財布手段から削除して対応する登録証のみを保管するようにしたものである。

【 0 0 2 4 】

本発明の請求項 1 0 に記載の発明は、請求項 3 記載の電子価値情報バックアッ

プシステムにおいて、暗号化手段が扱う暗号化方式を共通鍵方式として、暗号鍵と復号鍵に同じ鍵を用いるようにしたものである。

【0025】

本発明の請求項11に記載の発明は、請求項3記載の電子価値情報バックアップシステムにおいて、暗号化手段が扱う暗号化方式を公開鍵方式として、暗号鍵と復号鍵を非対称鍵とするようにしたものである。

【0026】

本発明の請求項12に記載の発明は、請求項4記載の電子価値情報バックアップシステムにおいて、鍵保管手段の所有者固有の情報を鍵管理手段に復号鍵と関連付けて所有者認証情報として登録することと、前記所有者固有の情報を鍵管理手段に提示して認証が成功した場合に前記復号鍵を前記鍵保管手段に復元するようにしたものである。

【0027】

本発明の請求項13に記載の発明は、請求項10記載の電子価値情報バックアップシステムにおいて、所有者認証情報として鍵保管手段とは独立したICカードに蓄積されたカード所有者を特定するための情報を用いるようにしたものである。

【0028】

本発明の請求項14に記載の発明は、請求項12記載の電子価値情報バックアップシステムにおいて、所有者認証情報として所有者の生体特徴情報を用いるようにしたものである。

【0029】

本発明の請求項15に記載の発明は、請求項12記載の電子価値情報バックアップシステムにおいて、鍵管理手段に対する所有者の正当性認証が成功した場合に、前記鍵管理手段が電子金庫手段と通信を行ない暗号化された電子価値情報を取得し、前記暗号化された電子価値情報の復号化を行なった電子価値情報を前記電子財布記憶手段上に復元するようにしたものである。

【0030】

本発明の請求項16に記載の発明は、請求項12記載の電子価値情報バックア

ップシステムにおいて、鍵管理手段に対して所有者の正当性認証が成功した場合に、前記鍵管理手段が電子金庫手段と通信を行ない暗号化された電子価値情報を取得し、前記暗号化された電子価値情報の復号化を行なった電子価値情報を新しく生成した暗号鍵を用いて暗号化し、前記の新しい暗号鍵で暗号化された前記電子価値情報を電子金庫上の古い暗号鍵で暗号化された前記電子価値情報と置き換え、前記鍵管理手段が新しい暗号鍵と復号鍵を鍵保管手段に配布するようにしたものである。

【0031】

本発明の請求項17に記載の発明は、請求項12記載の電子価値情報バックアップシステムにおいて、鍵管理手段に対して所有者の正当性認証が成功した場合に、前記鍵管理手段が電子金庫手段と通信を行ない暗号化された電子価値情報を取得し、前記暗号化された電子価値情報の復号化を行なった電子価値情報を新しく生成した暗号鍵を用いて暗号化し、前記の新しい暗号鍵で暗号化された前記電子価値情報を電子財布手段上に復元し、前記鍵管理手段が新しい暗号鍵と復号鍵を鍵保管手段に配布するようにしたものである。

【0032】

本発明の請求項18に記載の発明は、請求項12記載の電子価値情報バックアップシステムにおいて、電子財布手段が保管する電子価値情報に対して前記電子財布手段上のバックアップ条件情報と照合を行ない、条件に合致する電子価値情報を自動的に電子金庫手段に登録し登録証を受けとるようにしたものである。

【0033】

本発明の請求項19に記載の発明は、請求項18記載の電子価値情報バックアップシステムにおいて、バックアップ条件情報をユーザが変更できるようにしたものである。

【0034】

本発明の請求項20に記載の発明は、請求項18記載の電子価値情報バックアップシステムにおいて、バックアップ条件情報として、電子価値情報の種類を用いるようにしたものである。

【0035】

本発明の請求項 21 に記載の発明は、請求項 18 記載の電子価値情報バックアップシステムにおいて、バックアップ条件情報として、電子価値情報のサイズを用いるようにしたものである。

【0036】

本発明の請求項 22 に記載の発明は、請求項 18 記載の電子価値情報バックアップシステムにおいて、バックアップ条件情報として、電子価値情報のサイズと電子財布記憶手段の空きメモリ容量を用いるようにしたものである。

【0037】

本発明の請求項 23 に記載の発明は、請求項 18 記載の電子価値情報バックアップシステムにおいて、バックアップ条件情報として、電子価値情報の有効期限を用いるようにしたものである。

【0038】

本発明の請求項 24 に記載の発明は、請求項 18 記載の電子価値情報バックアップシステムにおいて、バックアップ条件情報として、電子価値情報の保持開始時間を用いるようにしたものである。

【0039】

本発明の請求項 25 に記載の発明は、請求項 1 記載の電子価値情報バックアップシステムにおいて、電子財布手段が登録証を提示して前記電子価値情報を前記電子財布手段上に復元する時、復元に十分な容量が電子財布上に残っていない場合、容量不足をユーザに対して提示し復元作業を中断するようにしたものである。

【0040】

本発明の請求項 26 に記載の発明は、請求項 1 記載の電子価値情報バックアップシステムにおいて、電子財布手段が登録証を提示して前記電子価値情報を前記電子財布手段上に復元する時または新規の電子価値情報を登録する時、復元や新規登録に十分な容量が電子財布記憶手段上に残っていない場合、電子財布手段上のバックアップ条件情報に基づいて現在保持されている電子価値情報を自動的に電子金庫手段に登録し登録証と置き換え、電子金庫上の電子価値情報を復元するための領域を空けることによって復元作業を継続するようにしたものである。

【 0 0 4 1 】

本発明の請求項 2 7 に記載の発明は、請求項 2 6 記載の電子価値情報バックアップシステムにおいて、電子財布手段が電子価値情報の登録証を提示して前記電子価値情報を前記電子財布手段上に復元する時または新規の電子価値情報を登録する時、復元や新規登録に十分な容量が電子財布記憶手段上に残っていない場合、処理の中断および処理継続の方法を提示して選択させることで、復元作業の中断もしくは継続するようにしたものである。

【 0 0 4 2 】

本発明の請求項 2 8 に記載の発明は、電子財布手段として、電子価値情報と登録証を保管する電子財布記憶手段を備え、電子金庫手段に対して通信を行うようにしたものである。

【 0 0 4 3 】

本発明の請求項 2 9 に記載の発明は、請求項 2 8 記載の電子財布手段において、登録証に電子価値情報の部分情報を含むようにしたものである。

【 0 0 4 4 】

本発明の請求項 3 0 に記載の発明は、電子財布手段として、電子価値情報と登録証を保管する電子財布記憶手段と、電子価値情報を暗号化する暗号鍵と、暗号化された電子情報を復号化する復号鍵とを有する暗号化手段を備え、電子金庫手段に対して通信を行うようにしたものである。

【 0 0 4 5 】

本発明の請求項 3 1 に記載の発明は、請求項 3 0 記載の電子財布手段において、請求項 3 0 の復号鍵を 2 つに分割した部分鍵の一方を電子価値情報と組にして電子金庫手段に登録するようにしたものである。

【 0 0 4 6 】

本発明の請求項 3 2 に記載の発明は、請求項 3 1 記載の電子財布手段において、請求項 3 1 の部分鍵を、暗号鍵と復号鍵を数学的に生成する元となった情報を 2 つに分割した一方とするようにしたものである。

【 0 0 4 7 】

本発明の請求項 3 3 に記載の発明は、請求項 2 8 記載の電子財布手段において

、前記電子金庫手段から送られた登録証が、バックアップする電子価値情報に対応する登録証であることを検証する登録証検証手段を備え、前記電子金庫手段から登録証を取得した際、前記登録証が前記バックアップする電子価値情報に対応する登録証であることが検証された場合に、前記登録証に対応する電子価値情報を電子財布記憶手段上から削除するようにしたものである。

【 0 0 4 8 】

本発明の請求項 3 4 に記載の発明は、請求項 2 8 記載の電子財布手段において、設定されたバックアップ条件情報との照合を行ない、条件に合致する電子価値情報を自動的に電子金庫手段に登録して登録証を取得するようにしたものである。

【 0 0 4 9 】

本発明の請求項 3 5 に記載の発明は、請求項 2 8 記載の電子財布手段において、電子価値情報の復元時または新規登録時に電子財布記憶手段上に十分な記憶容量が残っていない場合、容量不足をユーザに対して提示し復元作業を中断するようにしたものである。

【 0 0 5 0 】

本発明の請求項 3 6 に記載の発明は、請求項 2 8 記載の電子財布手段において、電子価値情報の復元時または新規登録時に電子財布記憶手段上に十分な記憶容量が残っていない場合、自動的にバックアップ条件情報に基づいて電子価値情報のバックアップを行って記憶容量を確保するようにしたものである。

【 0 0 5 1 】

本発明の請求項 3 7 に記載の発明は、請求項 2 8 記載の電子財布手段において、電子価値情報の復元時または新規登録時に電子財布記憶手段上に十分な記憶容量が残っていない場合、容量不足を提示して復元作業を中断するか自動的にバックアップ条件情報に基づいてバックアップを行なって記憶容量を確保するかをユーザに選択させるようにしたものである。

【 0 0 5 2 】

本発明の請求項 3 8 に記載の発明は、電子金庫手段として、電子価値情報を保管する電子金庫記憶手段を備え、電子価値情報から登録証を生成することと、登

録証に対応する電子価値情報を電子金庫記憶手段から引き出すようにしたものである。

【0053】

本発明の請求項39に記載の発明は、請求項38記載の電子金庫手段において、登録証に電子価値情報の部分情報が含まれるようにしたものである。

【0054】

本発明の請求項40に記載の発明は、請求項38記載の電子金庫手段において、暗号化された電子価値情報の登録を受けて登録証を生成し、登録証の提示を受けて暗号化された電子価値情報を返すようにしたものである。

【0055】

本発明の請求項41に記載の発明は、請求項40記載の電子金庫手段において、復号鍵を2つに分割した一方の部分鍵と暗号化した電子価値情報の登録を受けて登録証を生成し、登録証の提示を受けて暗号化された電子価値情報と部分鍵を返すようにしたものである。

【0056】

本発明の請求項42に記載の発明は、請求項41記載の電子金庫手段において、請求項41の部分鍵を、暗号鍵と復号鍵を数学的に生成する元となった情報を2つに分割した一方とするようにしたものである。

【0057】

本発明の請求項43に記載の発明は、鍵管理手段として、登録要求を受けた鍵を保管する鍵管理記憶手段を備えたものである。

【0058】

本発明の請求項44に記載の発明は、鍵管理手段として、登録要求を受けた鍵を認証情報と組にして保管する鍵管理記憶手段を備え、認証情報が一致する場合のみ前記鍵管理記憶手段上に登録された鍵を引き出すようにしたものである。

【0059】

本発明の請求項45に記載の発明は、鍵管理手段として、暗号鍵と復号鍵の鍵ペアを生成して鍵管理記憶手段上に保管するとともに暗号化手段に対して配布するようにしたものである。

【0060】

本発明の請求項 4 6 に記載の発明は、鍵管理手段として、電子金庫手段と通信して、電子金庫手段上の暗号化された電子価値情報を鍵管理記憶手段上の復号鍵を用いて復号し、新しく暗号鍵と復号鍵の鍵ペアを生成し、新しい暗号鍵を用いて前記電子価値情報を暗号化した電子価値情報を古い暗号化された電子価値情報との置き換えることを電子金庫手段に対して要求し、新しい鍵ペアを暗号化手段に配布するようにしたものである。

【0061】

本発明の請求項 4 7 に記載の発明は、鍵管理手段として、電子金庫手段と通信して、電子金庫手段上の暗号化された電子価値情報を鍵管理記憶手段上の復号鍵を用いて復号し、前記電子価値情報を電子財布手段に送るようにしたものである。

【0062】

本発明の請求項 4 8 に記載の発明は、暗号化手段として、鍵管理手段と通信して所有者認証に基づいて復号鍵の登録と取得を行なうことを特徴とする暗号化手段。

【0063】

本発明の請求項 4 9 に記載の発明は、暗号化手段として、電子金庫手段と通信して登録証と対応する一方の分割鍵を取得し、鍵管理手段と通信して所有者認証に基づいて他方の分割鍵を取得し、2つの分割鍵を用いて復号鍵を復元するようにしたものである。

【0064】

本発明の請求項 5 0 に記載の発明は、制御プログラム記録媒体として、請求項 1 から請求項 2 7 および請求項 2 8 から請求項 3 7 に記載の電子財布手段の制御プログラムを、電子計算機が読み取り可能な形式で記録したことを特徴とするものである。

【0065】

本発明の請求項 5 1 に記載の発明は、制御プログラム記録媒体として、請求項 1 から請求項 2 7 および請求項 3 7 から請求項 4 2 に記載の電子金庫手段の制御

プログラムを、電子計算機が読み取り可能な形式で記録したことを特徴とするものである。

【 0 0 6 6 】

本発明の請求項 5 2 に記載の発明は、制御プログラム記録媒体として、請求項 3 から請求項 2 7 および請求項 4 3 から請求項 4 7 に記載の鍵管理手段の制御プログラムを、電子計算機が読み取り可能な形式で記録したことを特徴とするものである。

【 0 0 6 7 】

本発明の請求項 5 3 に記載の発明は、制御プログラム記録媒体として、請求項 2 から請求項 2 7 および請求項 4 8 から請求項 4 9 に記載の暗号化手段の制御プログラムを、電子計算機が読み取り可能な形式で記録したことを特徴とするものである。

【 0 0 6 8 】

【発明の実施形態】

以下、図 1 から図 1 8 を用いて本発明の実施の形態について説明する。なお、本発明はこれらの実施の形態に何等限定されるものではなく、その要旨を逸脱しない範囲に置いて種々なる態様で実施し得る。

【 0 0 6 9 】

(実施の形態 1)

図 1 から 3 と図 7 を用いて、請求項 1 から請求項 2 と請求項 9 と請求項 2 8 から請求項 2 9 と請求項 3 3 と請求項 3 8 から請求項 3 9 との実施の形態について述べる。

【 0 0 7 0 】

図 1 は、本実施の形態が示す電子価値情報バックアップシステムの一例を示した構成図である。本システムは基本的に有線または無線の通信路によって結ばれたコンピュータ装置と、それに接続された外部拡張機器およびそれらの上で動作するソフトウェアで構成されるものとする。ここでいうコンピュータ装置とは、ソフトウェアプログラムにしたがって動作する CPU を備えた機器の総称を意味するものとする。

【0071】

本実施の形態では、電子財布手段101および電子財布記憶手段102はICカード121の中に構成される。端末100はICカードリーダーを備えた携帯電話端末であり、ICカード121内に構成された電子財布手段101と通信することが出来る。端末100と電子金庫手段103は、無線によって通信を行なう。なお、端末100は、ICカードリーダーを備えた、パーソナルコンピュータ、または、セットトップボックス、または、携帯型端末であっても良い。また、端末100と電子金庫手段103の間の通信は、有線通信であってもよい。また、電子財布手段101と電子財布記憶手段102をICカード中ではなく、端末100上に内蔵する形で構成してもよい。

【0072】

電子財布手段101はソフトウェアと前記ソフトウェア格納する記憶領域と前記ソフトウェアを解釈して実行するためのOSおよびCPUによって実現される。また、電子財布手段101は電子財布記憶手段102の内容の参照と変更を行なうことができる。電子財布記憶手段102はEEPROMなどの書き換え可能なメモリによって実現される。

【0073】

電子価値情報とは電子現金や電子チケットなどを表す電子情報であり、登録証とは前記電子価値情報を電子金庫手段103に登録したさいに発行される前記電子価値情報の控えを表す電子情報である。図3に電子財布記憶手段102での電子価値情報と登録証の管理方法を示す。電子財布手段101は電子財布記憶手段102上にインデックス851を置く。前記インデックス851は、電子財布記憶手段102上に格納された情報に対するポインタと前記情報のサイズとポインタの先の情報の種別を表す記号の組をまとめたものである。これにより、電子財布手段101は次に示す機能を実現できる。

【0074】

電子財布手段101は電子財布記憶手段102中のインデックス851を参照してポインタとサイズを取得し、取得したポインタとサイズを用いて電子価値情報または登録証を取り出すことができる。また、この電子財布手段101は電子

財布記憶手段102中のインデックス851を参照してすべてのポインタとサイズを取得し、それを用いて、すべての電子価値情報と登録証のタイトル情報を取得する。前記のポインタとサイズタイトルを用いて、全保管情報のリストを作成することができる。また、特定の条件に合致するポインタとサイズを取得することで、条件に合致する情報のリスト（例えば登録証のリストや有効期限完了まで残り一週間以内の情報のリストなど）を作成することもできる。

【0075】

電子財布手段101は、電子財布記憶手段102中の空き領域に電子価値情報または登録証を書き込み、それに対応する種別とポインタとサイズの組のエントリをインデックス851に追加することで、電子財布記憶手段102に電子価値情報または登録証を保管することができる。またその逆に、インデックス851中に示されたポインタとサイズを参照して、前記ポインタとサイズが指す領域を消去し、前記ポインタとサイズに対応したエントリをインデックス851から削除することで、電子財布記憶手段102から電子価値情報または登録証を削除することができる。また、新規登録と削除を組み合わせることで、電子価値情報または登録証の情報を修正することができる。なお、上記の仕組み或いは機能はICカード201上のオペレーティングシステム（OS）が持つ機能を用いて実現しても良い。

【0076】

電子金庫手段103はワークステーションまたはパーソナルコンピュータなどのコンピュータ装置と、前記コンピュータシステム上で動作するソフトウェアから構成される。電子金庫手段103は電子金庫記憶手段110の内容の参照と変更を行なうことができる。電子金庫記憶手段110は電子金庫手段103が内容の参照と変更を行なうことができる記憶装置であり、ハードディスクなどで実現される。電子金庫記憶手段110上には前記コンピュータシステムのOSが管理するファイルシステムが構築されている。図2（a）に電子価値情報の一例として電子価値情報201を示す。電子金庫手段103が電子価値情報201の登録要求を受けた場合、図2（c）に示す登録証301を電子価値情報201を用いて生成する。登録証301を生成する処理の流れを以下に説明する。

【0077】

電子金庫手段103は設定に基づいて、電子価値情報201から図2(b)に示すダイジェスト302を生成する。また、電子価値情報201を一方向性のハッシュ関数に通してX1という数を生成する。電子金庫手段103が持つカウンタを参照しY1という数を取得する。前記カウンタは参照の度に1ずつ昇順で増加し、上限に達すれば0に戻るものであるとする。これらダイジェスト302とハッシュ値X1とカウンタ値Y1を組として登録証301とする。前記X1を生成するために用いたハッシュ関数として、MD5やSHA1などの分散性の高いものを用いることとする。なお、ダイジェスト302は空情報であってもよい。

【0078】

図7に電子金庫記憶手段110での情報の保管方法を示す。電子金庫記憶手段110は、電子価値情報201をファイル801、登録証301をファイル802として保管する。登録証301の構成要素であるハッシュ値X1とカウンタ値Y1とファイル801のパス情報とファイル802のパス情報を組として、インデックスファイル852の1つのエントリとして登録する。インデックスファイル852は1エントリ1行のCSVファイルであり、各行はカウンタ値によって昇順にソートされている。端末100から電子金庫手段103に登録証が提示された場合に、インデックスファイル852から登録証に対応する電子価値情報をカウンタ値の一致するエントリ群を検索し、その中からハッシュ値が一致するエントリ群にさらに絞り込み、登録証が完全に一致するエントリを抽出する。これにより登録証に対応する電子価値情報を高速に検索することが可能である。

【0079】

ユーザが端末100を操作して電子価値情報201をバックアップする手順を、以上に示した各手段を用いて示す。以下の手順での選択動作はすべてユーザによって行なわれる。

(1-1) 端末100が、電子財布手段101に電子価値情報リストを要求する。電子財布手段101は電子価値情報のリストを生成し、端末100に送る。

(1-2) 端末100が、電子価値情報リストから選択した電子価値情報201を電子財布手段101に要求する。電子財布手段101は電子価値情報201を電子

財布記憶手段102から取得し、端末100に送る。

(1-3) 端末100が、電子価値情報201の登録を電子金庫手段103に要求する。電子金庫手段103は電子価値情報201を電子金庫記憶手段110に保管すると同時に、電子価値情報201から登録証301を生成し、登録証301を端末100に送る。

(1-4) 端末100が、登録証301の保管を電子財布手段101に要求する。電子財布手段101は、電子価値情報201の内容と登録証301のダイジェスト302とを、電子価値情報201をハッシュ演算した値と登録証301のハッシュ値X1とを、それぞれ照合し、一致した場合に、登録証301を電子財布記憶手段102に保管し、完了通知を端末100に送る。一致しなかった場合には、電子財布手段101は、電子価値情報201のバックアップを中止し、エラー通知を端末100に送る。

【0080】

なお、登録証301が正常に電子財布記憶手段102に保管された場合、電子財布記憶手段102上から電子価値情報201を削除してもよい。ICカードのように記憶容量が少ないデバイスを用いる場合、これは記憶容量を効率的に利用する有効な手段である。

【0081】

同様に、ユーザが端末100を操作して電子財布記憶手段102に保管された登録証301に対応する電子価値情報201を電子財布記憶手段102上に復元する手順を次に示す。

(2-1) 端末100が、電子財布手段101に登録証リストを要求する。電子財布手段101は登録証リストを生成し、端末100に送る。

(2-2) 端末100が、登録証リストから選択した登録証301を電子財布手段101に要求する。電子財布手段101は登録証301を電子財布記憶手段102から取得し、端末100に送る。

(2-3) 端末100が、電子金庫手段103に登録証301を提示し、対応する電子価値情報の取得を要求する。電子金庫手段103は登録証301を用いて電子価値情報201を検索して取得し、端末100に送る。この時、電子金庫手段1

03は、検索した電子価値情報の内容と登録証301とを照合し、不整合がたった場合には、電子価値情報201の復元処理を中止する。

(2-4) 端末100が、電子価値情報201の登録を電子財布手段101に要求する。電子財布手段101は電子価値情報201を電子財布記憶手段102に保管し、完了通知を取得する。

【0082】

以上に説明したシステムを用いることで、ユーザが持つ電子価値情報を電子金庫記憶手段上にバックアップすることと、バックアップした電子価値情報の概要を電子金庫手段に問い合わせることなく知ることと、必要に応じて電子価値情報を電子財布記憶手段上に復元することが可能となる。

【0083】

【実施の形態2】

図4から6を用いて、請求項3と請求項5と請求項10から11と請求項30と請求項40の実施の形態について述べる。図4は本実施の形態における電子価値情報バックアップシステムの一例を示した構成図であり、本システムは実施の形態1（図1）で示されたシステムの端末100を端末112に置き換え、電子金庫手段103を電子金庫手段113に置き換え、ICカード121をICカード122と置き換えたものである。ICカード122はICカード121に対して暗号化手段105と鍵保管手段104を追加し、電子財布手段101を電子財布手段111に変更したものである。

【0084】

暗号化手段105は、ソフトウェアと前記ソフトウェアを格納する記憶領域と前記ソフトウェアを解釈して実行するためのOSおよびCPUによって構成される。鍵保管手段104はEEPROMなどの書き換え可能なメモリによって実現される。なお、暗号化手段105と電子財布手段111はOSとCPUを共有してもよい。また、鍵保管手段104と電子財布記憶手段102はEEPROMを共有してもよい。

【0085】

鍵保管手段104は暗号鍵401と復号鍵402を保持する（図6）。本実施

の形態では、鍵保管手段104に保管された暗号鍵401と復号鍵402のペアは、暗号化手段105が生成する。暗号化手段105は公開鍵暗号方式を用いることとし、暗号鍵401を公開鍵、復号鍵402を秘密鍵とする。なお、暗号化手段105の暗号化方式として共有鍵暗号方式を用いてもよい。その場合、暗号鍵401と復号鍵402は同一の鍵となる。

【0086】

暗号化手段105は、鍵保管手段104から暗号鍵401を取得し、電子価値情報201を入力として電子価値情報202を生成する。図5は登録電子価値情報203を示したものである。登録電子価値情報203は、ダイジェスト302と、電子価値情報201を暗号鍵401で暗号化した暗号化電子価値情報202と、ダイジェスト302と暗号化電子価値情報202をまとめて暗号鍵401で電子署名した署名303から構成される。暗号化手段105は、鍵保管手段104から復号鍵402を取得し、登録電子価値情報203を入力として電子価値情報201を再生する。暗号化手段105は復号鍵402を用いて署名303を検証して正当性が確認した後、暗号化電子価値情報202を復号化して電子価値情報201を生成する。

【0087】

電子財布手段111は実施の形態1の電子財布手段101の持つ機能をすべて持つと同時に、暗号化手段105に対して電子価値情報を渡して登録電子価値情報を生成することと、登録電子価値情報を渡して電子価値情報を生成することを要求する機能を持つ。

【0088】

電子金庫手段113は電子金庫手段103のソフトウェアを変更したものであり、電子金庫手段113は電子金庫記憶手段110の内容の参照と変更を行なうことができる。電子金庫103が登録電子価値情報203の登録要求を受けた場合、図5(b)に示す登録証304を登録電子価値情報203を用いて生成する。登録証304を生成する処理の流れを以下に説明する。また、電子金庫手段113は、登録電子価値情報203からダイジェスト302を抽出する。また、暗号化電子価値情報202を一方向性のハッシュ関数に通してX2という数を生成

する。電子金庫手段 113 が持つカウンタを参照し Y2 という数を取得する。前記カウンタは参照の度に 1 ずつ昇順で増加し、上限に達すれば 0 に戻るものであるとする。これらダイジェスト 302 とハッシュ値 X2 とカウンタ値 Y2 を組として登録証 304 とする。前記 X2 を生成するために用いたハッシュ関数として、MD5 や SHA1 などの分散性の高いものを用いることとする。登録証 304 はダイジェスト 302 の情報を含むため、それを参照することで登録された電子価値情報の概要を把握する事ができる。なお、ダイジェスト 302 は空情報の場合であってもよいが、その場合は登録証からデンスカチジョウホウの概要を知る事はできない。

【0089】

ユーザが端末 112 を操作して電子価値情報 201 をバックアップする手順を示す。以下の手順での選択動作はすべてユーザによって行なわれる。

(1-1) 端末 112 が、電子財布手段 111 に電子価値情報リストを要求する。電子財布手段 111 は電子価値情報のリストを生成し、端末 112 に送る。

(1-2) 端末 112 が、電子価値情報リストから選択した電子価値情報 201 を電子財布手段 111 に要求する。電子財布手段 111 は電子価値情報 201 を電子財布記憶手段 102 から取得する。暗号化手段 105 は電子価値情報 201 から登録電子価値情報 203 を生成し、電子財布手段 111 に送る。電子財布手段 111 は登録電子価値情報 203 を端末 112 に送る。

(1-3) 端末 112 が、登録電子価値情報 203 の登録を電子金庫手段 113 に要求する。電子金庫手段 113 は登録電子価値情報 203 を電子金庫記憶手段 110 に保管すると同時に、登録電子価値情報 203 から登録証 304 を生成し、登録証 304 を端末 112 に送る。

(1-4) 端末 112 が、登録証 304 の保管を電子財布手段 111 に要求する。電子財布手段 111 は登録証 304 を電子財布記憶手段 102 に保管し、完了通知を端末 112 に送る。

【0090】

同様に、ユーザが端末 112 を操作して電子財布記憶手段 102 に保管された登録証 304 に対応する電子価値情報 201 を電子財布記憶手段 102 上に復元

する手順を次に示す。

(2-1) 端末 112 が、電子財布手段 111 に登録証リストを要求する。電子財布手段 111 は登録証リストを生成し、端末 112 に送る。

(2-2) 端末 112 が、登録証リストから選択した登録証 304 を電子財布手段 111 に要求する。電子財布手段 111 は登録証 304 を電子財布記憶手段 102 から取得し、端末 112 に送る。

(2-3) 端末 112 が、電子金庫手段 113 に登録証 304 を提示し、対応する登録電子価値情報を要求する。電子金庫手段 113 は登録証 304 を用いて登録電子価値情報 203 を検索して取得し、端末 112 に送る。

(2-4) 端末 112 が、登録電子価値情報 203 の登録を電子財布手段 111 に要求する。電子財布手段 111 は登録電子価値情報 203 を暗号化手段 105 に送り、電子価値情報 201 を取得し、電子財布記憶手段 102 に保管し、完了通知を取得する。

【0091】

以上に説明したシステムを用いることで、ユーザが持つ電子価値情報を電子金庫手段には秘密の鍵を用いて暗号化してバックアップすることと、バックアップした電子価値情報の概要をローカルで把握することと、必要に応じて暗号化してバックアップした電子価値情報を電子金庫手段から復元することが可能となる。

【0092】

【実施の形態 3】

図 8 から 9 を用いて、請求項 4 と請求項 6 と請求項 12 と請求項 43 から請求項 44 と請求項 48 の実施の形態について述べる。図 8 は本実施の形態における電子価値情報バックアップシステムの一例を示した構成図であり、本システムは実施の形態 2（図 4）で示されたシステムの端末 112 を端末 114 に変更し、IC カード 122 を IC カード 123 に変更して暗号化手段 105 を暗号化手段 115 に変更し、鍵管理手段 106 を追加したものである。

【0093】

端末 114 と暗号化手段 115 はそれぞれ、端末 112 と暗号化手段 105 の間で通信を行なえるように変更したものであり、それを除いた機能は端末 112

と暗号化手段 105 と同様である。鍵管理手段 106 はワークステーションまたはパーソナルコンピュータなどのコンピュータ装置と、前記コンピュータシステム上で動作するソフトウェアから構成される。鍵管理手段 106 は鍵管理記憶手段 116 の内容の参照と変更を行なうことができる。鍵管理記憶手段 116 は鍵管理手段 106 が内容の参照と変更を行なうことができる記憶装置であり、ハードディスクなどで実現される。鍵管理記憶手段 116 上には前記コンピュータシステムの OS が管理するファイルシステムが構築されている。

【0094】

図 9 に鍵管理記憶手段 116 での情報の保管方法を示す。鍵管理記憶手段 116 は、鍵情報 491 をファイル 803、認証情報 891 をファイル 804 として保管する。ファイル 803 へのパスとファイル 804 へのパスと前記認証情報のハッシュ値を組として、インデックスファイル 853 の 1 つのエントリとして登録する。インデックスファイル 853 は 1 エントリ 1 行の CSV ファイルであり、各行はハッシュ値によって昇順にソートされている。端末 114 から鍵管理手段 106 に認証情報 891 が提示された場合に、インデックスファイル 853 から認証情報 891 のハッシュ値に一致するエントリ群を検索し、その中から認証情報が完全に一致するエントリを抽出する。これにより、認証情報 891 に対応する鍵情報 491 を検索することが可能である。

【0095】

本実施の形態では、前記の認証情報 891 として端末 114 から入力したパスワードを用いる。なお、認証情報 891 として、IC カード 123 の固有 ID、または鍵保管手段 104 が保持する暗号鍵 401 を用いて復号鍵 402 を暗号化したものを用いても良い。

【0096】

電子価値情報のバックアップと復元の仕組みは実施の形態 2 と同様であるので説明を省略する。例えば、鍵保管手段 104 に保持されている復号鍵 402 をバックアップする鍵情報 491 とした場合の鍵情報 491 のバックアップと復元の手順について説明する。なお、鍵情報 491 として、暗号鍵 401 と復号鍵 402 の組を用いてもよい。

【0097】

ユーザが端末114を操作して復号鍵402をバックアップする手順を示す。

以下の手順での選択動作はすべてユーザによって行なわれる。

(1-1) 端末114が暗号化手段115に対して復号鍵の取得を要求する。

(1-2) 暗号化手段115が鍵保管手段104を参照し、復号鍵402を取得する

。

(1-3) 暗号化手段115が端末114に復号鍵402を渡す。

(1-4) 端末114が認証情報891を取得する。本実施の形態ではパスワード入力をユーザに行なわせる。

(1-5) 端末114が復号鍵402を鍵管理手段106に認証情報891とともに登録することを要求する。

(1-6) 鍵管理手段106が復号鍵402と認証情報891を組として鍵管理記憶手段116に保管する。

(1-7) 鍵管理手段106が端末114に登録完了を通知する。

【0098】

同様に、ユーザが端末114を操作して鍵管理記憶手段116に保管された復号鍵4402を鍵保管手段104に復元する手順を次に示す。

(2-1) 端末114が認証情報891を取得する。本実施の形態ではパスワード入力をユーザに行なわせる。

(2-2) 端末114が鍵管理手段106に認証情報891を提示して、復号鍵の取得を要求する。

(2-3) 鍵保管手段106は認証情報に対応する復号鍵402を鍵管理記憶手段116から抽出し、端末114に渡す。

(2-4) 端末114が復号鍵402を暗号化手段105に送る。

(2-5) 暗号化手段115が復号鍵402を鍵保管手段104に保管する。

(2-6) 暗号化手段115が復号鍵の復元が完了したことを端末100に通知する

。

【0099】

なお、暗号鍵401と復号鍵402の鍵ペアを鍵管理手段106で生成し、鍵

保管手段 1 0 4 に配布してもよい。この場合、復号鍵の 4 0 2 のバックアップは鍵ペアの配布時に同時に行なわれる。この場合の鍵ペア配布の手順は次の通りである。

(3-1) 端末 1 1 4 が認証情報 8 9 1 を取得する。

(3-2) 端末 1 1 4 が認証情報 8 9 1 を鍵管理手段 1 0 6 に送るとともに、暗号鍵と復号鍵の新規生成を要求する。

(3-3) 鍵管理手段 1 0 6 が、暗号鍵 4 0 1 と復号鍵 4 0 2 を生成する。

(3-4) 鍵管理手段 1 0 6 が、復号鍵 4 0 2 と認証情報 8 9 1 を組として鍵管理記憶手段 1 1 6 に保管する。

(3-5) 鍵管理手段 1 0 6 が、暗号鍵 4 0 1 と復号鍵 4 0 2 の鍵ペアを端末 1 1 4 に送る。(3-6) 端末 1 1 4 が暗号化手段 1 1 5 に前記鍵ペアを鍵保管手段 1 0 4 に登録することを要求する。

(3-7) 暗号化手段 1 1 5 が鍵保管手段 1 0 4 に前記鍵ペアを保管する。

(3-8) 暗号化手段 1 1 5 が端末 1 1 4 に前記鍵ペアの保管完了を通知する。

【 0 1 0 0 】

以上に説明したシステムを用いることで、ユーザが持つ電子価値情報を電子金庫手段には秘密の鍵を用いて暗号化してバックアップすることと、バックアップした電子価値情報の概要をローカルで把握することと、必要に応じて暗号化してバックアップした電子価値情報を電子金庫手段から復元することと、前記の暗号化を解読する復号鍵を紛失した場合にも認証が成功すればその鍵を鍵保管手段上に復元することで暗号化された電子価値情報を復号することが可能となる。

【 0 1 0 1 】

【実施の形態 4】

図 1 7 から 1 8 を用いて、請求項 7 から 8 と請求項 3 1 から請求項 3 2 と請求項 4 1 から請求項 4 2 と請求項 4 9 の実施の形態について述べる。図 1 7 は本実施の形態に置ける電子価値情報バックアップシステムの一例を示した構成図であり、本システムは実施の形態 3 (図 8) で示されたシステムの端末 1 1 4 を端末 1 4 1 に置き換え、電子金庫手段 1 1 3 を電子金庫手段 1 4 2 に置き換え、IC カード 1 2 3 を IC カード 1 2 5 に置き換え、電子財布手段 1 1 1 を電子財布手

段 139 に変更し、暗号化手段 115 を暗号化手段 140 に変更したものである。

【0102】

暗号化手段 140 は、暗号化手段 115 の鍵情報バックアップと復元の仕組みを変更したものであり、鍵情報のバックアップと復元時に、電子財布手段 139 と連携するようにしたものである。

【0103】

電子金庫手段 142 は、電子金庫手段 113 が電子金庫記憶手段 110 に保管し管理するデータのデータ形式を変更したものである。そのデータ形式の例を図 18 の登録電子価値情報 204 に示す。この登録電子価値情報 204 は、電子財布手段 139 から電子価値情報 201 を受けとった暗号化手段 140 が生成する。鍵情報が正常な場合の電子価値情報をバックアップから電子財布記憶手段に復元する手順は、実施の形態 3 と同様である。

【0104】

本実施の形態での鍵情報のバックアップの手順は、実施の形態 3 での鍵情報バックアップの手順を変更し、鍵管理手段 106 にバックアップする鍵情報 491 を分割復号鍵 405 としたものである。

(1-1) 端末 141 が暗号化手段 140 に対して復号鍵の取得を要求する。

(1-2) 暗号化手段 140 が鍵保管手段 104 を参照し、復号鍵 402 を取得する。

(1-3) 暗号化手段 140 が、復号鍵 402 を 2 つに分割して分割復号鍵 405 と分割復号鍵 406 を生成する。

(1-4) 暗号化手段 140 が端末 141 に分割復号鍵 405 を渡す。

(1-5) 端末 141 が認証情報 891 を取得する。本実施の形態ではパスワード入力をユーザに行なわせる。

(1-6) 端末 141 が分割復号鍵 405 を鍵管理手段 106 に認証情報 891 とともに登録することを要求する。

(1-7) 鍵管理手段 106 が分割復号鍵 405 と認証情報 891 を組として鍵管理記憶手段 116 に保管する。

(1-8) 鍵管理手段 106 が端末 141 に登録完了を通知する。

【0105】

本実施の形態での電子価値情報のバックアップの手順は、実施の形態 2 での電子価値情報のバックアップの手順を変更したものである。その手順を以下に示す。

(2-1) 端末 141 が、電子財布手段 139 に電子価値情報リストを要求する。電子財布手段 139 は電子価値情報のリストを生成し、端末 141 に送る。

(2-2) 端末 141 が、電子価値情報リストから選択した電子価値情報 201 を電子財布手段 139 に要求する。電子財布手段 139 は電子価値情報 201 を電子財布記憶手段 102 から取得する。暗号化手段 105 は電子価値情報 201 から登録電子価値情報 204 を生成し、電子財布手段 139 に送る。電子財布手段 139 は登録電子価値情報 204 を端末 141 に送る。

(2-3) 端末 141 が、登録電子価値情報 204 の登録を電子金庫手段 142 に要求する。電子金庫手段 142 は登録電子価値情報 204 を電子金庫記憶手段 110 に保管すると同時に、登録電子価値情報 204 から登録証 304 を生成し、登録証 304 を端末 141 に送る。

(2-4) 端末 141 が、登録証 304 の保管を電子財布手段 139 に要求する。電子財布手段 139 は登録証 304 を電子財布記憶手段 102 に保管し、完了通知を端末 141 に送る。

【0106】

本実施の形態での鍵情報の復元手順を以下に示す。

(3-1) 端末 141 が認証情報 891 を取得する。本実施の形態ではパスワード入力をユーザに行なわせる。

(3-2) 端末 141 が鍵管理手段 106 に認証情報 891 を提示して、分割復号鍵の取得を要求する。

(3-3) 鍵保管手段 106 は認証情報に対応する分割復号鍵 405 を鍵管理記憶手段 116 から抽出し、端末 141 に渡す。

(3-4) 端末 141 が分割復号鍵 405 を暗号化手段 140 に送る。

(3-5) 端末 141 が、電子財布手段 139 に登録証リストを要求する。電子財布

手段 139 は登録証リストを生成し、端末 141 に送る。

(3-6) 端末 141 が、登録証リストから選択した登録証 304 を電子財布手段 139 に要求する。電子財布手段 139 は登録証 304 を電子財布記憶手段 102 から取得し、端末 141 に送る。

(3-7) 端末 141 が、電子金庫手段 142 に登録証 304 を提示し、対応する登録電子価値情報を要求する。電子金庫手段 142 は登録証 304 を用いて登録電子価値情報 204 を検索して取得し、端末 141 に送る。

(3-8) 端末 141 が、登録電子価値情報 204 を電子財布手段 139 に送る。電子財布手段 139 は登録電子価値情報 204 から分割復号鍵 406 を取りだし、暗号化手段 104 に送る。

(3-9) 暗号化手段 140 が分割復号鍵 405 と分割復号鍵 406 を合成し、復号鍵 402 を取得する。

(3-10) 暗号化手段 140 が復号鍵 402 を鍵保管手段 104 に保管する。

(3-11) 暗号化手段 140 が復号鍵の復元が完了したことを端末 141 に通知する。

【0107】

なお、本実施の形態では、復号鍵を分割したものの一方をそれぞれを鍵管理記憶手段 116 に登録し、残りを電子金庫記憶手段 110 上の登録電子価値情報の中に埋め込むことによって鍵情報を分散してバックアップしている。復号鍵を分割したものをもちいるのではなく、復号鍵を数学的に生成するために用いる元の情報、例えば 2 つの素数をそれぞれ分割鍵として、一方を鍵管理記憶手段 116 に保管し、もう一方を電子金庫記憶手段 110 上の登録電子価値情報の中に埋め込むようにし、鍵の復元時に二つの情報をあわせて、暗号化手段 140 上で復号鍵を生成しなおすという方法を用いてもよい。この方法の場合、分割して保管した両方の元情報がわかって、暗号化方式や鍵を生成するために用いるパラメータがわからない限り、鍵を生成することができない。

【0108】

以上に説明したシステムを用いることで、ユーザが持つ電子価値情報を電子金庫手段には秘密の鍵を用いて暗号化してバックアップすることと、バックアップ

した電子価値情報の概要をローカルで把握することと、必要に応じて暗号化してバックアップした電子価値情報を電子金庫手段から復元することと、前記の暗号化を解読する復号鍵を紛失した場合にもその鍵を復元することと、鍵管理手段および電子金庫手段の共謀がなければそのどちらに対しても完全な復号鍵を知られないことと、鍵管理手段と電子金庫手段の共謀があっても暗号化方式と鍵の生成方法を知られない限り復号鍵を知られないことと、暗号化した電子価値情報を電子財布手段上に復元することが可能となる。

【0109】

【実施の形態5】

図10を用いて、請求項13から14の実施の形態について述べる。図10は本実施の形態に置ける電子価値情報バックアップシステムの一例を示した構成図であり、本システムは実施の形態2（図4）で示されたシステムの端末112を端末117に置き換え、認証手段118を追加したものである。本実施の形態は、実施の形態2において認証情報891として端末か112から入力されたパスワードを用いているのを、認証手段118から入力された認証情報を用いるように変更したものである。

【0110】

認証手段118はICカードリーダーを持ち、前記ICカードリーダーを用いて、ICカード122とは異なる個人認証用ICカードからICカード所有者情報を取得する。前記ICカード所有者情報を認証情報891として用いる。前記の個人認証用ICカードとしては、運転免許証やパスポートなどの行政などが発行する信頼できるカードを用いる。なお、認証手段118が指紋読みとり装置を持ち、前記指紋読みとり装置がユーザ指紋情報を取得し、前記ユーザ指紋情報を認証情報891として用いてもよい。また、認証手段118がICカードリーダーと指紋読みとり装置をともに持ち、ICカード所有者情報とユーザ指紋情報の組を認証情報891として用いてもよい。なお、指紋読みとり装置は、掌紋読みとり装置や網膜読みとり装置などの生体情報読みとり装置と置き換えてもよい。

【0111】

以上に説明したシステムを用いることで、ユーザが持つ電子価値情報を電子金

庫手段には秘密の鍵を用いて暗号化してバックアップすることと、バックアップした電子価値情報の概要をローカルで把握することと、必要に応じて暗号化してバックアップした電子価値情報を電子金庫手段から復元することと、前記の暗号化を解読する復号鍵を紛失した場合にも認証が成功すればその鍵を鍵保管手段上に復元することで暗号化された電子価値情報を復号することと、安全な方法で認証を実現することが可能となる。

【0112】

【実施の形態6】

図11を用いて、請求項15と請求項45の実施の形態について述べる。図11は本実施の形態における電子価値情報バックアップシステムの一例を示した構成図であり、本システムは実施の形態5（図10）で示されたシステムの鍵管理手段106を鍵管理手段119に置き換え、電子金庫手段113を電子金庫手段131に置き換え、端末117を端末132に置き換えたものである。

【0113】

本実施の形態では、鍵管理手段119と電子金庫手段131はお互いに通信する。これによって、実施の形態5に対して、鍵保管手段104から復号鍵を紛失したような緊急時に電子価値情報をバックアップから復元する新しい方法が追加される。

【0114】

同様に、ユーザが端末132を操作して電子財布記憶手段102に保管された登録証304に対応する電子価値情報201を電子財布記憶手段102上に復元する手順を次に示す。以下、復元したい電子価値情報を電子価値情報201、対応する登録証を登録証301、電子金庫上での電子価値情報201に対応する暗号化電子価値情報である暗号化電子価値情報202を含んだ登録電子価値情報を電子価値情報203、前記暗号化電子価値情報の復号に必要な復号鍵を復号鍵402として説明する。

(1-1) 端末132が、登録証301を電子財布手段111から取得する（詳細の手順は実施の形態2と同様である）。

(1-2) 端末132が、認証情報891とともに登録証301を鍵管理手段119

に送る。(1-3) 鍵管理手段 1 1 9 が、認証情報 8 9 1 に対応する復号鍵 4 0 2 を鍵管理記憶手段 1 1 6 から抽出する。対応する鍵が見つからない場合はエラー通知を端末 1 3 2 に送る。

(1-4) 鍵管理手段 1 1 9 が、電子金庫手段 1 3 1 に登録証 3 0 1 に対応する登録電子価値情報の取得を要求する。

(1-5) 電子金庫手段 1 3 1 が、電子金庫記憶手段 1 1 0 から登録証 3 0 1 に対応する登録電子価値情報 2 0 3 を抽出する。

(1-6) 電子金庫手段 1 3 1 が、登録電子価値情報 2 0 3 を鍵管理手段 1 1 9 に返す。

(1-7) 鍵管理手段 1 1 9 が、登録電子価値情報 2 0 3 内の署名 3 0 3 を復号鍵 4 0 2 を用いて検証し、暗号化電子価値情報 2 0 2 を復号鍵 4 0 2 を用いて復号し、電子価値情報 2 0 1 を取得する。

(1-8) 鍵管理手段 1 1 9 が、電子価値情報 2 0 1 を端末 1 3 2 に返す。

(1-9) 端末 1 3 2 が、電子財布手段 1 1 1 に電子価値情報 2 0 1 を電子財布記憶手段 1 0 2 に登録することを要求する。

(1-10) 電子財布手段 1 1 1 が電子価値情報 2 0 1 を電子財布記憶手段 1 0 2 に登録し、復元の完了を端末 1 3 2 に通知する。

【 0 1 1 5 】

なお、電子価値情報 2 0 1 の復元が完了した時に、対応する登録証 3 0 1 を削除してもよい。

【 0 1 1 6 】

以上に説明したシステムを用いることで、ユーザが持つ電子価値情報を電子金庫手段には秘密の鍵を用いて暗号化してバックアップすることと、バックアップした電子価値情報の概要をローカルで把握することと、必要に応じて暗号化してバックアップした電子価値情報を電子金庫手段から鍵管理手段を経由して鍵管理手段上で復号化してから復元することと、前記の暗号化を解読する復号鍵を紛失した場合にもその鍵を復元することで暗号化した電子価値情報を復元することと、鍵保管手段の正当性を所有者と強く結び付けることと、正当な所有者以外が不正に復号鍵を鍵保管手段に復元できないこと、正当な所有者以外が不正に電子価

値情報を復元できないことと、暗号化してバックアップした電子価値情報を維持しつつ暗号鍵と復号鍵の鍵ペアを変更することと、鍵保管手段の破損による場合の復号鍵の復元が可能となる。

【0117】**【実施の形態7】**

図12を用いて、請求項16と請求項46の実施の形態について述べる。図12は本実施の形態における電子価値情報バックアップシステムの一例を示した構成図であり、本システムは実施の形態6（図11）で示されたシステムの鍵管理手段113を鍵管理手段134に置き換え、端末132を端末133に置き換えたものである。

【0118】

本実施の形態における電子価値情報のバックアップと復元、復号鍵のバックアップと復元は、実施の形態3と同様である。本実施の形態は、鍵保管手段104上の暗号鍵と復号鍵がともに破損・消失した場合に、電子金庫手段131にバックアップされている電子価値情報を鍵管理手段134が取得し、鍵管理記憶手段134に登録されている復号鍵を用いて復号化する。鍵管理手段134は新しく暗号鍵と復号鍵の鍵ペアを生成し、前記暗号鍵を用いて電子価値情報を暗号化しなおし、新しい鍵ペアを端末133を経由して鍵保管手段104上に配布する。以下にその詳細の手順を示す。

- (1-1) 端末133が、全登録証群を電子財布手段111から取得する。
- (1-2) 端末133が、認証情報891とともに前記全登録証群を鍵管理手段134に送る。
- (1-3) 鍵管理手段119が、認証情報891に対応する復号鍵402を鍵管理記憶手段116から抽出する。対応する鍵が見つからない場合はエラー通知を端末134に送る。
- (1-4) 鍵管理手段134が、電子金庫手段131に前記全登録証群に対応する暗号化電子価値情報すべての取得を要求する。
- (1-5) 電子金庫手段131が、電子金庫記憶手段110から前記全登録証群に対応する暗号化電子価値情報群を抽出する。

(1-6) 電子金庫手段 1 3 1 が、登録電子価値情報群を鍵管理手段 1 3 4 に返す。

(1-7) 鍵管理手段 1 3 4 が、登録電子価値情報群に含まれるすべての暗号化電子価値情報を復号鍵 4 0 2 を用いて復号し、電子価値情報群を取得する。

(1-8) 鍵管理手段 1 3 4 が、暗号鍵 4 0 3 と復号鍵 4 0 4 の鍵ペアを生成する。

(1-9) 鍵管理手段 1 3 4 が、暗号鍵 4 0 3 で全電子価値情報群を暗号化し、新しい暗号化電子価値情報群を生成し、登録電子価値情報群に含まれる署名も新しい暗号鍵で生成し直し置き換える。

(1-10) 鍵管理手段 1 3 4 が、新しい登録電子価値情報群を(1-5)で取得した登録電子価値情報群との置き換えることを電子金庫手段 1 3 1 に要求する。

(1-11) 電子金庫手段 1 3 1 が、古い登録電子価値情報群を新しい登録電子価値情報群で置き換え、その置換えの完了を鍵管理手段 1 3 4 に通知する。

(1-12) 鍵管理手段 1 3 4 が、鍵管理記憶手段 1 1 6 上に保管された復号鍵 4 0 2 を復号鍵 4 0 4 に置き換える。

(1-13) 鍵管理手段 1 3 4 が、暗号鍵 4 0 3 と復号鍵 4 0 4 の鍵ペアを端末 1 3 3 に送る。

(1-14) 端末 1 3 3 が、暗号化手段 1 1 5 に前記鍵ペアを鍵保管手段 1 0 4 に保管するよう要求する。

(1-15) 暗号化手段 1 1 5 が、鍵保管手段 1 0 4 に前記鍵ペアを保管し、その完了を通知する。

【 0 1 1 9 】

以上に説明したシステムを用いることで、ユーザが持つ電子価値情報を電子金庫手段には秘密の鍵を用いて暗号化してバックアップすることと、バックアップした電子価値情報の概要をローカルで把握することと、必要に応じて暗号化してバックアップした電子価値情報を電子金庫手段から鍵管理手段を経由して鍵管理手段上で復号化してから復元することと、前記の暗号化を解読する復号鍵を紛失した場合にもその鍵を復元することで暗号化した電子価値情報を復元することと、鍵保管手段の正当性を所有者と強く結び付けることと、正当な所有者以外が不正に復号鍵を鍵保管手段に復元できないこと、正当な所有者以外が不正に電子価値情報を復元できないことと、暗号化してバックアップした電子価値情報を維持

しつづ暗号鍵と復号鍵の鍵ペアを変更することと、鍵保管手段の破損による場合の復号鍵の復元が可能となる。

【0120】

【実施の形態8】

図13を用いて、請求項17と請求項47の実施の形態について述べる。図13は本実施の形態における電子価値情報バックアップシステムの一例を示した構成図であり、本システムは実施の形態6（図11）で示されたシステムの鍵管理手段134を鍵管理手段136に置き換え、端末133を端末135に置き換えたものである。

【0121】

本実施の形態の鍵管理手段136は、実施の形態6の鍵管理手段134が復号化した電子価値情報を端末133経由で送っていたのとは違い、新しく生成した暗号鍵で暗号化した状態で電子価値情報を端末135経由で送り、新しい暗号鍵と復号鍵を配布することを特徴としている。

(1-1) 端末135が、全登録証群を電子財布手段111から取得する。

(1-2) 端末135が、認証情報891とともに前記全登録証群を鍵管理手段136に送る。

(1-3) 鍵管理手段119が、認証情報891に対応する復号鍵402を鍵管理記憶手段116から抽出する。対応する鍵が見つからない場合はエラー通知を端末135に送る。

(1-4) 鍵管理手段136が、電子金庫手段131に前記全登録証群に対応する暗号化電子価値情報すべての取得を要求する。

(1-5) 電子金庫手段131が、電子金庫記憶手段110から前記全登録証群に対応する暗号化電子価値情報群を抽出する。

(1-6) 電子金庫手段131が、登録電子価値情報群を鍵管理手段136に返す。

(1-7) 鍵管理手段136が、登録電子価値情報群中の署名を検証した後、すべての暗号化電子価値情報を復号鍵402を用いて復号し、電子価値情報群を取得する。

(1-8) 鍵管理手段136が、暗号鍵403と復号鍵404の鍵ペアを生成する。

(1-9) 鍵管理手段 136 が、暗号鍵 403 で全電子価値情報群を暗号化し、新しく暗号化電子価値情報群を生成する。

(1-10) 鍵管理手段 136 が、鍵管理記憶手段 116 上に保管された復号鍵 402 を復号鍵 404 に置き換える。

(1-11) 鍵管理手段 136 が、暗号鍵 403 と復号鍵 404 の鍵ペアを端末 135 に送る。

(1-12) 鍵管理手段 136 が、電子金庫手段 131 上の(1-5)で取得した暗号化電子価値情報群を含む登録電子価値情報群の削除を要求する。

(1-13) 電子金庫手段 131 が、要求された登録電子価値情報群を削除し、その完了を鍵管理手段 136 に通知する。

(1-14) 鍵管理手段 136 が、新しい暗号化電子価値情報群を端末 135 に送る。

(1-15) 端末 135 が、新しい暗号化電子価値情報群と前記鍵ペアを暗号化手段 115 に送る。

(1-16) 暗号化手段 115 が前記鍵ペアを鍵保管手段 104 に保管する。

(1-17) 暗号化手段 115 が新しい暗号化電子価値情報群を復号鍵 404 で復号化し、電子財布手段 111 に電子価値情報群を送る。

(1-18) 電子財布手段 111 が電子価値情報群を電子財布記憶手段 102 上に復元する。(1-19) 電子財布手段 111 が端末 135 に完了を通知する。

【0122】

以上に説明したシステムを用いることで、ユーザが持つ電子価値情報を電子金庫手段には秘密の鍵を用いて暗号化してバックアップすることと、バックアップした電子価値情報の概要をローカルで把握することと、必要に応じて暗号化してバックアップした電子価値情報を電子金庫手段から鍵管理手段を経由して鍵管理手段上で復号化してから復元することと、前記の暗号化を解読する復号鍵を紛失した場合にもその鍵を復元することで暗号化した電子価値情報を復元することと、鍵保管手段の正当性を所有者と強く結び付けることと、正当な所有者以外が不正に復号鍵を鍵保管手段に復元できないこと、正当な所有者以外が不正に電子価値情報を復元できないことと、暗号化してバックアップした電子価値情報を維持

しつづ暗号鍵と復号鍵の鍵ペアを変更することと、鍵保管手段の破損による場合の復号鍵の復元が可能となる。

【0123】

【実施の形態9】

図14から16を用いて、請求項18から27と請求項34から請求項37の実施の形態について述べる。

【0124】

図14は本実施の形態が示す電子価値情報バックアップシステムの一例を示した構成図である。これは実施の形態3のICカード123をICカード124に変更したものであり、ICカード124はICカード123の電子財布手段111を電子財布手段138に変更し、電子財布手段138と通信するバックアップ起動管理手段109を追加したものである。これによってバックアップする電子価値情報の選択を、ユーザによる手動選択ではなく事前に設定した条件に基づいて自動的に行なうようにしたものである。

【0125】

バックアップ起動管理手段109は、バックアップ条件情報を保持し、その条件情報に基づいて、バックアップする電子価値情報を決定する。本実施の形態では、バックアップ条件情報には初期設定が存在し、また条件情報をユーザが変更できるものとし、電子財布記憶手段102の空きメモリ容量、電子価値情報の有効期限、電子価値情報の種類、電子価値情報のサイズのそれぞれを組み合わせるバックアップ条件を設定することができるものとする。なお、電子価値情報が持つ情報の項目にあわせて、前記した以外の情報をバックアップ条件に用いても良い。

【0126】

バックアップ条件情報の例を図15と図16で示す。図15は電子記憶手段上の電子価値情報群の例である。ここでバックアップ条件を映画のチケットとした場合、図16(a)は前記バックアップ条件に対応する電子価値情報群を示す。本日の日付を2000年3月15日として、一ヶ月以内に使用可能な日がないことをバックアップ条件とした場合の対応する電子価値情報群は図16(b)が示され

る。

【0127】

図39はバックアップ起動管理手段109が管理するバックアップ条件をユーザが設定する手順を示した図であり、以下に示す番号順に実行される。以下の番号は、図39における番号と対応している。

- (1-1) 端末137がバックアップ起動手段109の現在のバックアップ条件を取得し、ユーザに提示する。
- (1-2) ユーザはバックアップ条件を修正し、新しいバックアップ条件を生成する。
- (1-3) 端末137がバックアップ起動手段109に新しいバックアップ条件を登録する。

【0128】

図40はバックアップ手順を示した図であり、以下に示す番号順に実行される。以下の番号は、図40における番号と対応する。

- (2-1) (2-1)バックアップ起動管理手段109が電子財布手段11に電子価値情報のリストを要求する。
- (2-2) (2-2)電子財布手段138が電子財布記憶手段102を参照し、電子価値情報のリストを構成する。
- (2-3) (2-3)電子財布手段138が電子価値情報のリストをバックアップ起動管理手段109に返す。
- (2-4) (2-4)バックアップ起動管理手段109は登録されたバックアップ条件とリストを照合し、バックアップ対象電子価値情報リストを生成する。
- (2-5) (2-5)バックアップ起動管理手段109は電子財布手段138にバックアップ対象電子価値情報リストを渡す。
- (2-6) (2-6)電子財布手段138は電子財布記憶手段102からバックアップ対象電子価値情報リストで指定された電子価値情報群を取得する。
- (2-7) (2-7)前記電子価値情報群に含まれるすべての電子価値情報をそれぞれ暗号化手段115を用いて暗号化し、暗号化電子価値情報群を生成する。
- (2-8) (2-8)前記暗号化電子価値情報群に含まれるすべての暗号化電子価値情報

を端末 1 3 7 を経由して、電子金庫手段 1 1 3 にバックアップする。

(2-9) (2-9)電子金庫手段 1 1 3 から前記暗号化電子価値情報群に対応する登録証群を端末 1 3 7 を経由して電子財布手段 1 3 8 に渡す

(2-10) (2-10)電子財布手段 1 3 8 は前記登録証群を電子財布記憶手段 1 0 2 に保管し、電子財布記憶手段 1 0 2 上から前記電子価値情報群に含まれる電子価値情報をすべて削除する。

(2-11) (2-11)電子財布記憶手段 1 3 8 は端末 1 3 7 に完了を通知する。

【 0 1 2 9 】

(2-8)、(2-9)、(2-10)での 1 つの暗号化電子価値情報に対しての手順の細部は、前述した実施の形態 3 と同様であるので、本実施の形態では詳細の説明を省略する。

【 0 1 3 0 】

なお、一定時間ごとにバックアップ起動管理手段 1 0 9 が自動的に前記(2-1)から(2-11)で示した手順に従ってバックアップを開始してもよい。

【 0 1 3 1 】

または新規の電子価値情報が電子財布記憶手段に登録される時やバックアップされていた電子価値情報を復元する時に、電子財布記憶手段 1 0 2 の記憶容量が不足する場合にバックアップ起動管理手段 1 0 9 が自動的に前記手順にしたがってバックアップを開始してもよい。

【 0 1 3 2 】

またはユーザによる起動要求があった場合に、バックアップ起動管理手段 1 0 9 が自動的に前記手順にしたがってバックアップを開始してもよい。

【 0 1 3 3 】

または、前記の条件の組み合わせによって、バックアップ起動管理手段 1 0 9 が自動的に前記手順にしたがってバックアップを開始してもよい。

【 0 1 3 4 】

また、電子財布記憶手段の記憶容量不足の場合、現在の電子財布記憶手段に保持された電子価値情報をバックアップ条件情報に基づいてバックアップする処理を行なった上で新規の電子価値情報の登録やバックアップ済みの電子価値情報の

復元を継続することと、新規の電子価値情報の登録やバックアップ済み電子価値情報の復元を中断することと、手動で現在の電子財布記憶手段に保持された電子価値情報を選択しバックアップする処理を行なった上で新規の電子価値情報の登録やバックアップ済みの電子価値情報の復元を継続することを端末 1 3 7 を操作するユーザに選択させても良い。

【0 1 3 5】

以上に説明したシステムを用いることで、ユーザが持つ電子価値情報を電子金庫手段には秘密の鍵を用いて暗号化してバックアップすることと、バックアップした電子価値情報の概要をローカルで把握することと、必要に応じて暗号化してバックアップした電子価値情報を電子金庫手段から復元することと、前記の暗号化を解読する復号鍵を紛失した場合にもその鍵を復元することで暗号化した電子価値情報を復元することと、鍵保管手段の正当性を所有者と強く結び付けることと、正当な所有者以外が不正に復号鍵を鍵保管手段に復元できないことと、鍵保管手段の破損による場合の復号鍵の復元することと、工場設定やユーザ設定に基づいて電子価値情報のバックアップが自動的に起動させることが可能となる。

【0 1 3 6】

【発明の効果】

以上のように本発明によれば、第 1 にローカルの電子価値情報を暗号化してサーバ上にバックアップする手段を備えたことにより、電子価値情報をサーバに隠蔽した状態でバックアップすることと、ローカルの電子価値情報が破損した場合にも電子価値情報を復元する効果が得られる。

【0 1 3 7】

第 2 に暗号化した電子価値情報の復号鍵を電子価値情報のバックアップ先のサーバとは別のサーバにバックアップする手段を備えたことにより、ローカルの復号鍵が破損した場合にも復号鍵を復元する事によって暗号化した電子価値情報を復元する効果が得られる。

【0 1 3 8】

第 3 に復号鍵を分割してそれぞれを別々にバックアップする手段を備えた事により、復号鍵の全体を知られる事なく、ローカルに復号鍵を復元する効果が得ら

れる。

【0139】

第4に復号鍵をバックアップしたサーバに、暗号化した電子価値情報を復号させて電子価値情報をローカルに復元する手段を備えた事により、ローカルデバイスが壊滅的に破損または紛失した場合にも、電子価値情報を復元する効果が得られる。

【0140】

第5に復号鍵をバックアップしたサーバに、暗号化した電子価値情報を復号させ、新しい暗号化を行なわせて登録しなおし、新しい鍵情報をローカル環境に再配布させる手段を備えたことにより、ローカル環境の鍵情報のみが破損または紛失した場合にも、ローカル環境に与える影響を小さく抑えた上でバックアップした電子価値情報を復元できる環境を再構築する効果が得られる。

【図面の簡単な説明】

【図1】

本発明の実施の形態1の電子価値情報バックアップシステムの構成を示すブロック図

【図2】

実施の形態1の電子価値情報とダイジェスト情報と登録証の例図

【図3】

実施の形態1の電子財布手段上での電子価値情報と登録証の管理方法の例図

【図4】

本発明の実施の形態2の電子価値情報バックアップシステムの構成を示すブロック図

【図5】

実施の形態2の登録電子価値情報と登録証の例図

【図6】

実施の形態2の鍵保管手段上での暗号鍵と復号鍵の保管方法の例図

【図7】

実施の形態1の電子金庫記憶手段での情報の保管方法の例図

【図 8】

本発明の実施の形態 3 の電子価値情報バックアップシステムの構成を示すブロック図

【図 9】

実施の形態 3 の鍵管理記憶手段上の鍵情報の管理方法の例図

【図 1 0】

本発明の実施の形態 5 の電子価値情報バックアップシステムの構成を示すブロック図

【図 1 1】

本発明の実施の形態 6 の電子価値情報バックアップシステムの構成を示すブロック図

【図 1 2】

本発明の実施の形態 7 の電子価値情報バックアップシステムの構成を示すブロック図

【図 1 3】

本発明の実施の形態 8 の電子価値情報バックアップシステムの構成を示すブロック図

【図 1 4】

本発明の実施の形態 9 の電子価値情報バックアップシステムの構成を示すブロック図

【図 1 5】

実施の形態 9 の電子価値情報群の例図

【図 1 6】

実施の形態 9 のバックアップ対象の電子価値情報群の例図

【図 1 7】

実施の形態 4 の鍵管理記憶手段上の鍵情報の管理方法の例図

【図 1 8】

実施の形態 4 の登録電子価値情報と登録証の例図

【符号の説明】

100 端末

101 電子財布手段

102 電子財布記憶手段

103 電子金庫手段

104 鍵保管手段

105 暗号化手段

106 鍵管理手段

109 バックアップ起動管理手段

110 電子金庫記憶手段

111 電子財布手段

112 端末

113 電子金庫手段

114 端末

115 暗号化手段

116 鍵管理記憶手段

117 端末

118 認証手段

119 鍵管理手段

121 101と102を含むICカード

122 102と104と105と111を含むICカード

123 102と104と115と111を含むICカード

124 102と104と109と115と138を含むICカード

125 102と104と139と140を含むICカード

131 電子金庫手段

132 端末

133 端末

134 鍵管理手段

135 端末

136 鍵管理手段

137 端末

138 電子財布手段

139 電子財布手段

140 暗号化手段

141 端末

142 電子金庫手段

201 電子価値情報例

202 201に対応した暗号化電子価値情報例

203 202に対応した登録電子価値情報例

204 204と406に対応した登録電子価値情報例

301 201に対応した登録証

302 201に対応したダイジェスト例

303 203に含まれる署名

304 203に対応した登録証

401 暗号鍵例

402 復号鍵例

403 暗号鍵例

404 復号鍵例

405 402の分割復号鍵

406 402の分割復号鍵

491 鍵情報

801 電子金庫記憶手段上のファイル例

802 電子金庫記憶手段上のファイル例

803 鍵管理記憶手段上のファイル例

804 鍵管理記憶手段上のファイル例

851 電子財布記憶手段上のインデックス例

852 電子金庫記憶手段上のインデックスファイル例

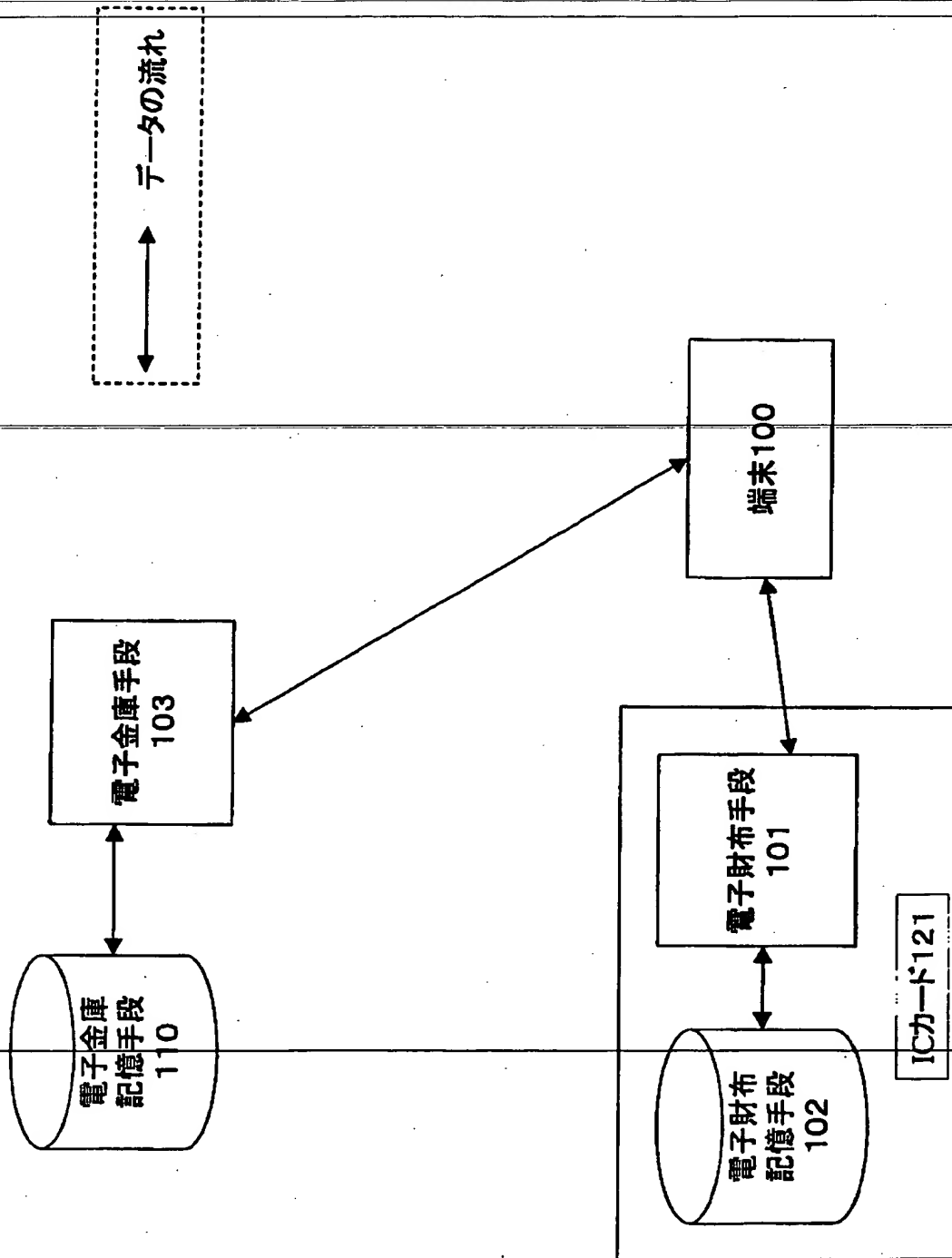
853 電子金庫記憶手段上のインデックスファイル例

91 認証情報例

【書類名】

図面

【図 1】



【図 2】

電子価値情報201

情報種別	映画チケット
名前	映画タイトル
単価	A円
数	B
合計金額	A×B円
場所	劇場名
有効期限	C～D
備考

(a) ダイジェスト302

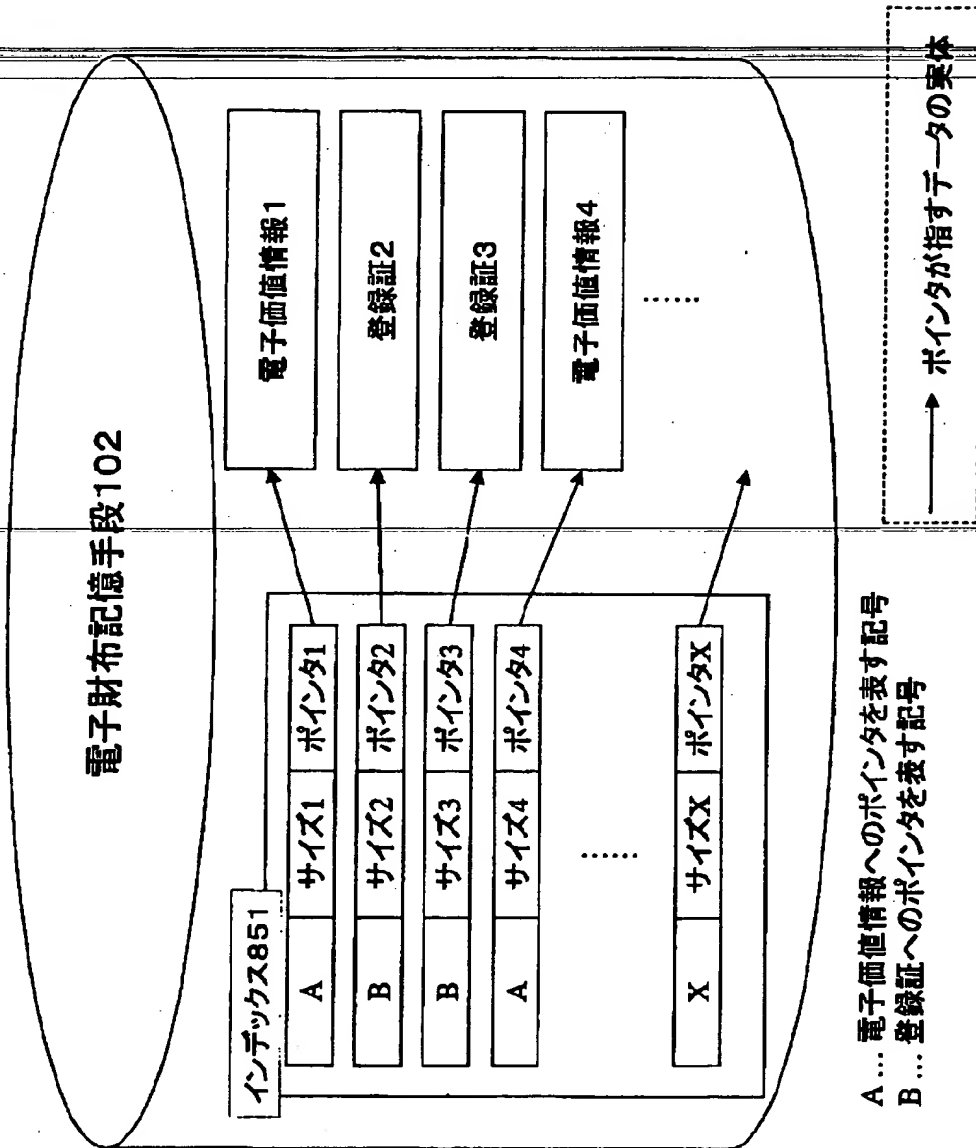
情報種別	映画チケット
名前	映画タイトル
数	B
有効期限	C～D
場所	劇場名

(b) 登録証301

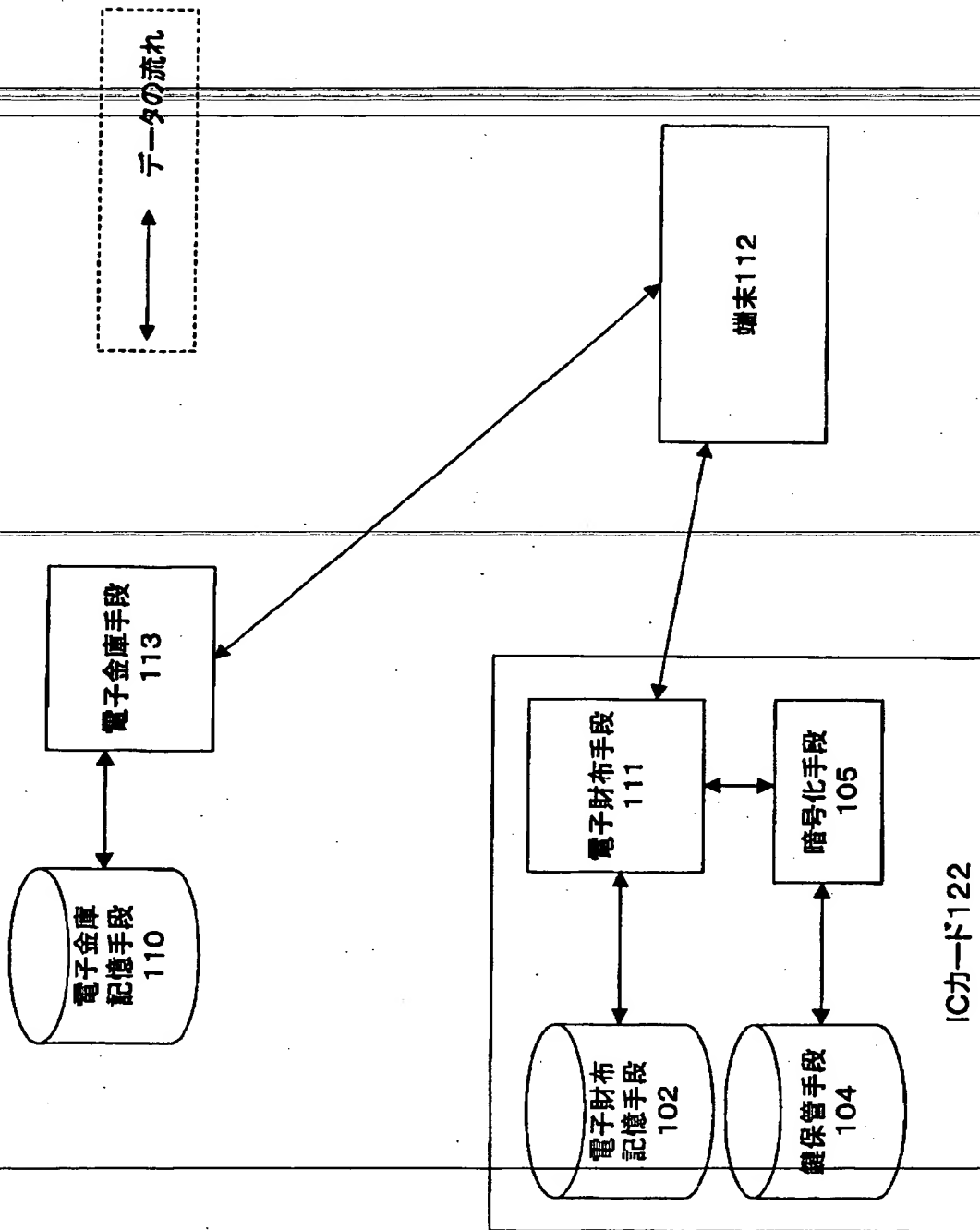
ダイジェスト302	ハッシュ値X1	カウンタ値Y1
-----------	---------	---------

(c)

【図 3】



【図 4】



【図 5】

登録電子価値情報203

情報種別	映画チケット
名前	映画タイトル
数	B
場所	劇場名
有効期限	C~D
ダイジェスト302	
暗号化電子価値情報202	
署名303	

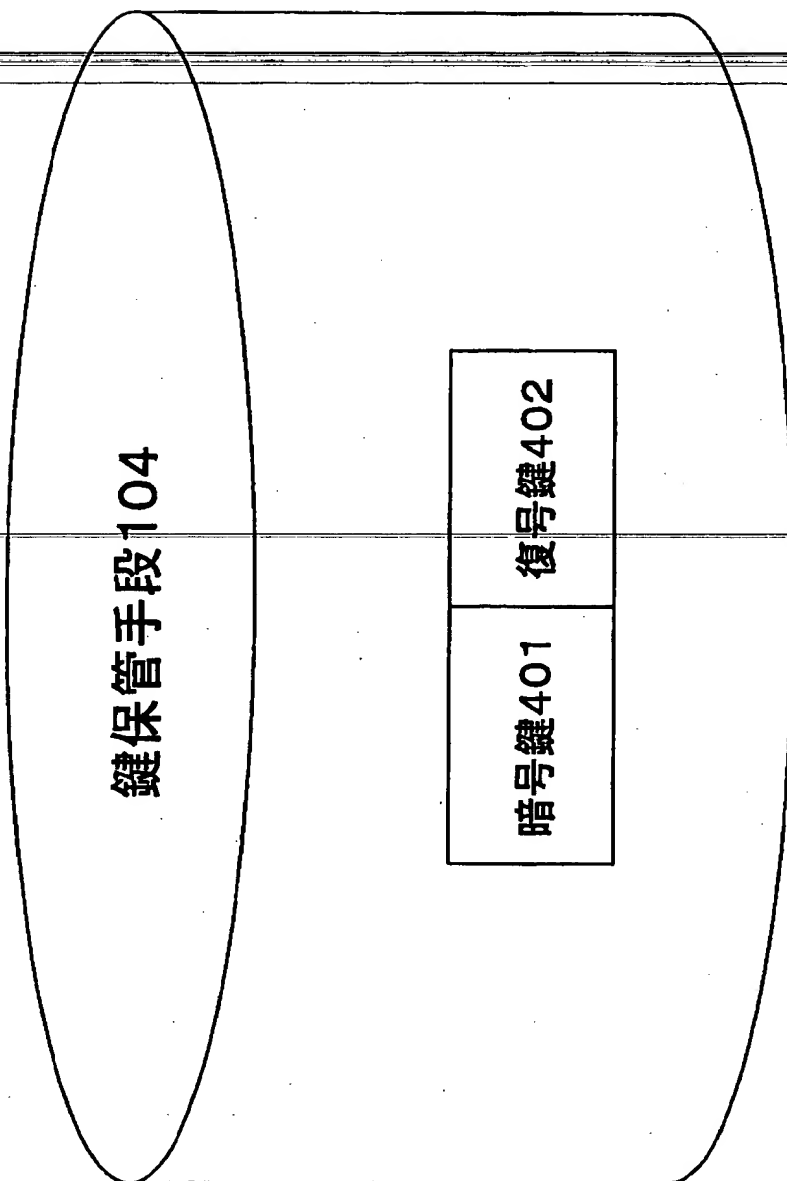
(a)

登録証304

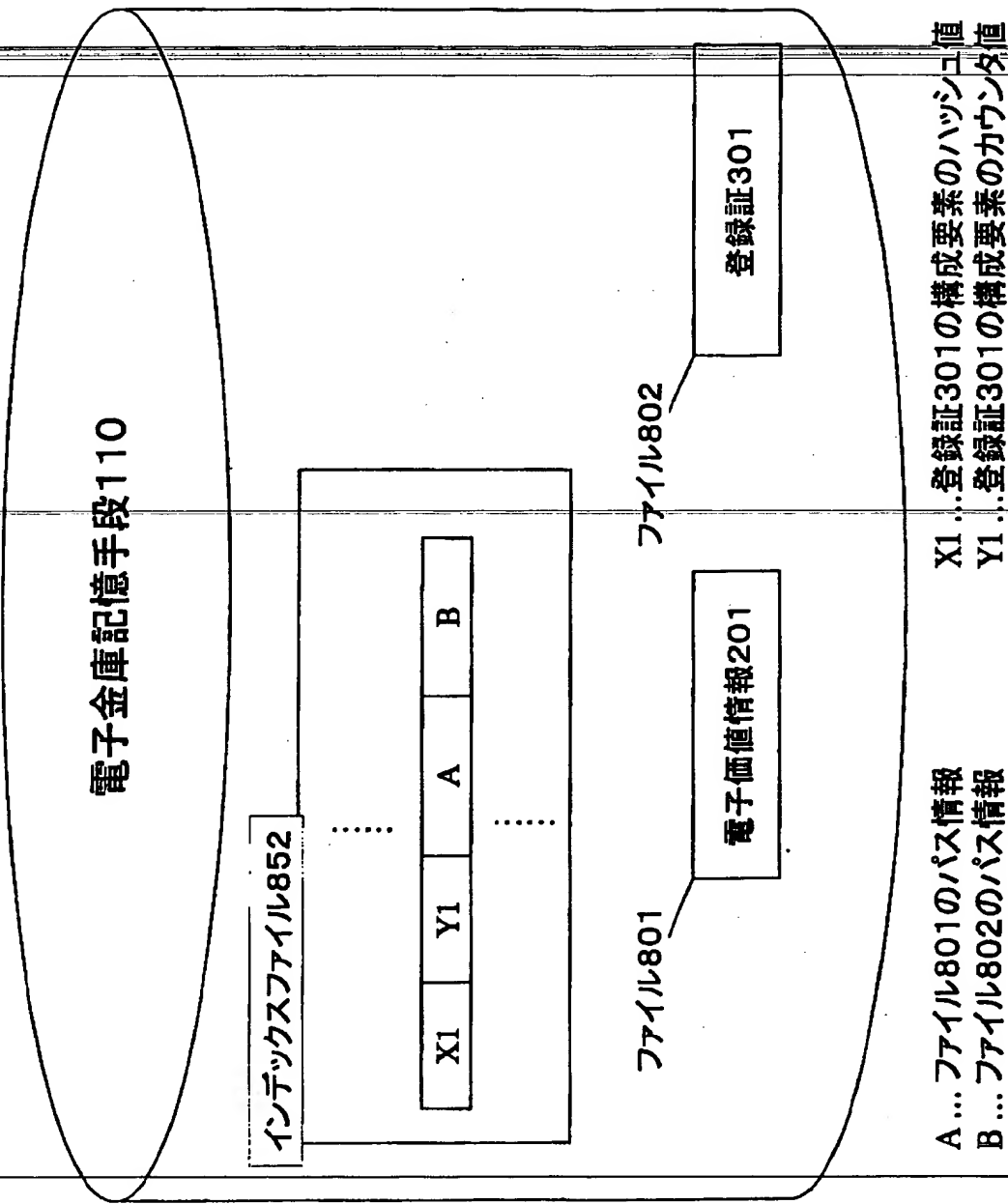
ダイジェスト302	ハッシュ値X2	カウンタ値Y2
-----------	---------	---------

(b)

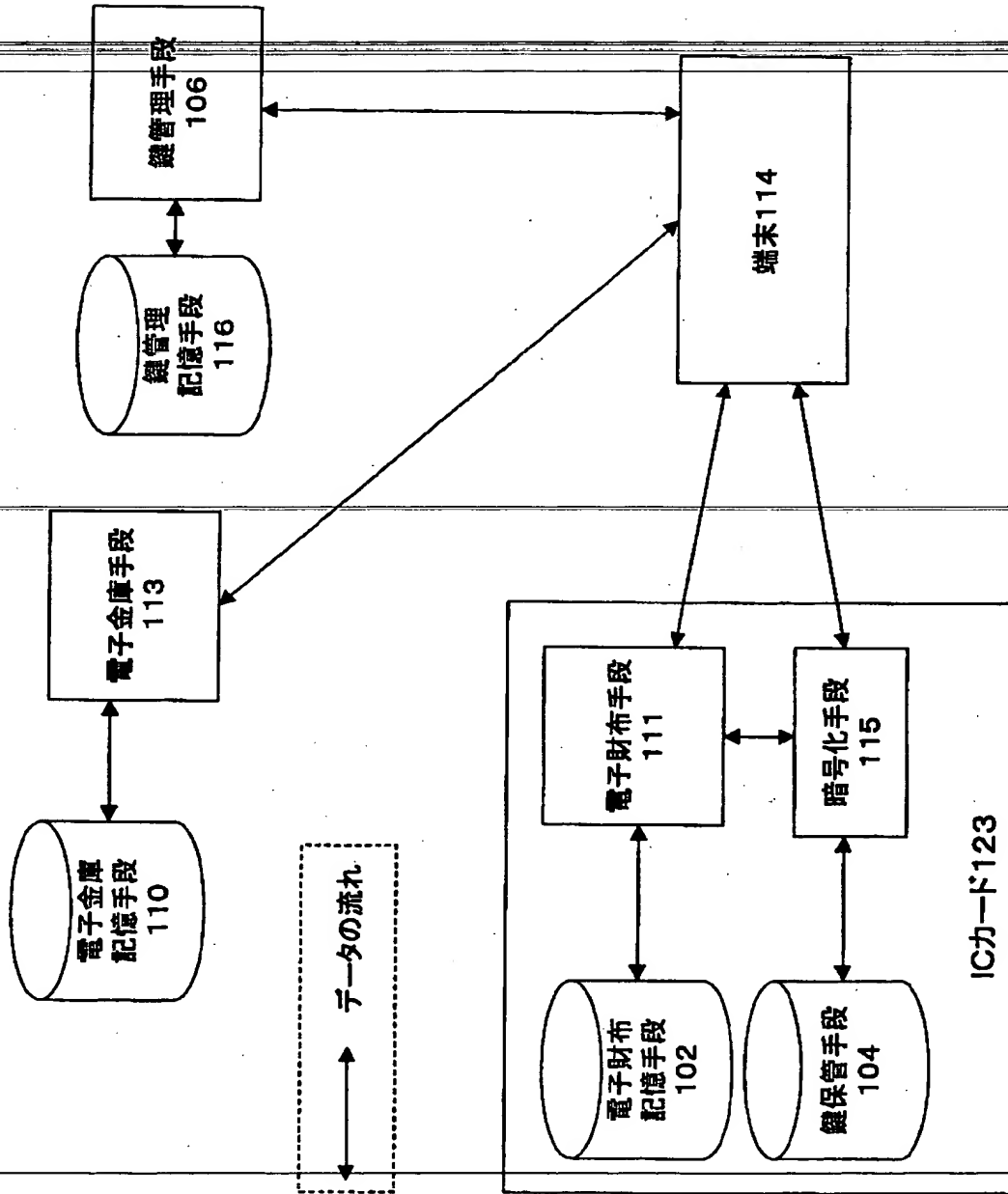
【図 6】



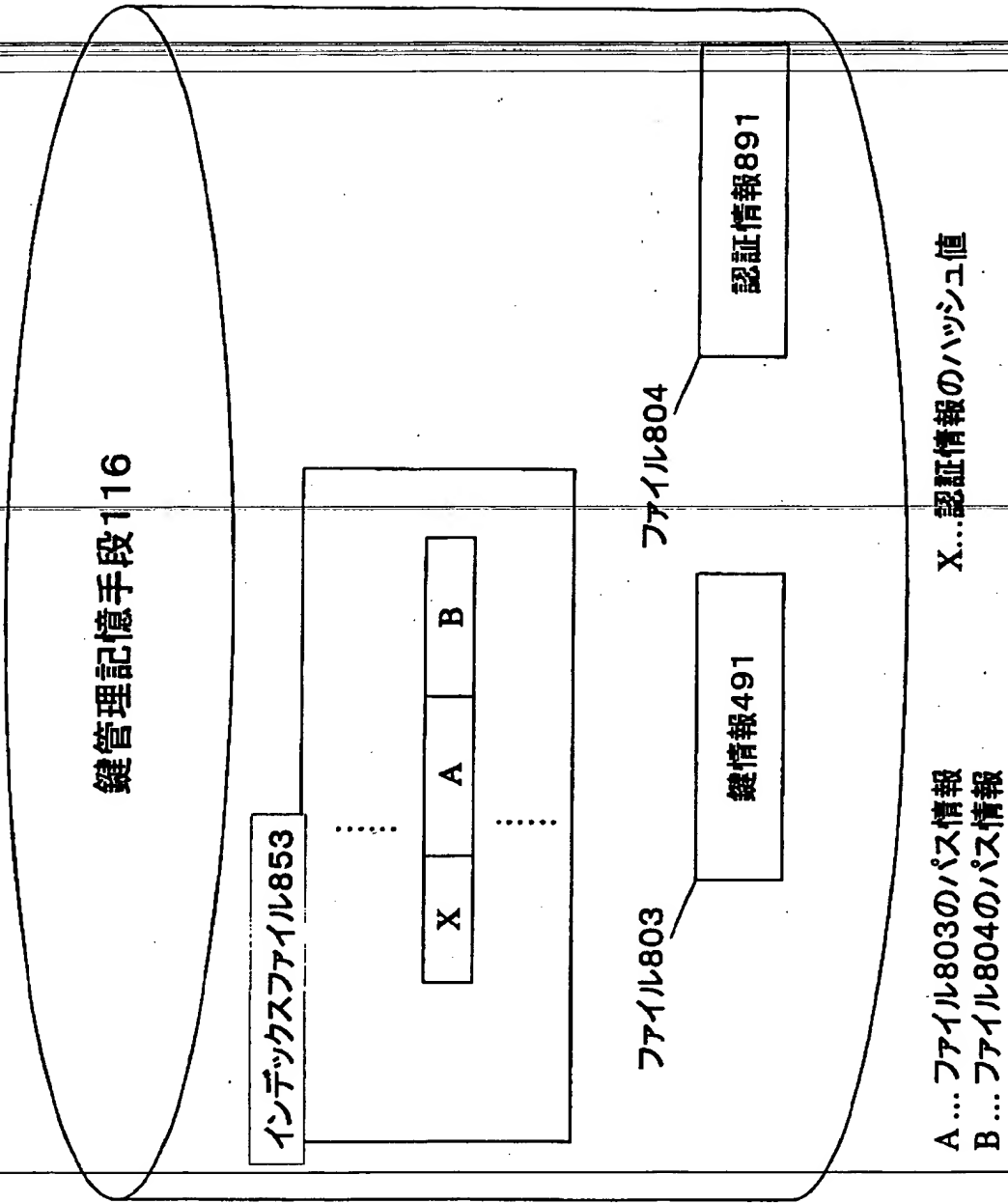
【図 7】



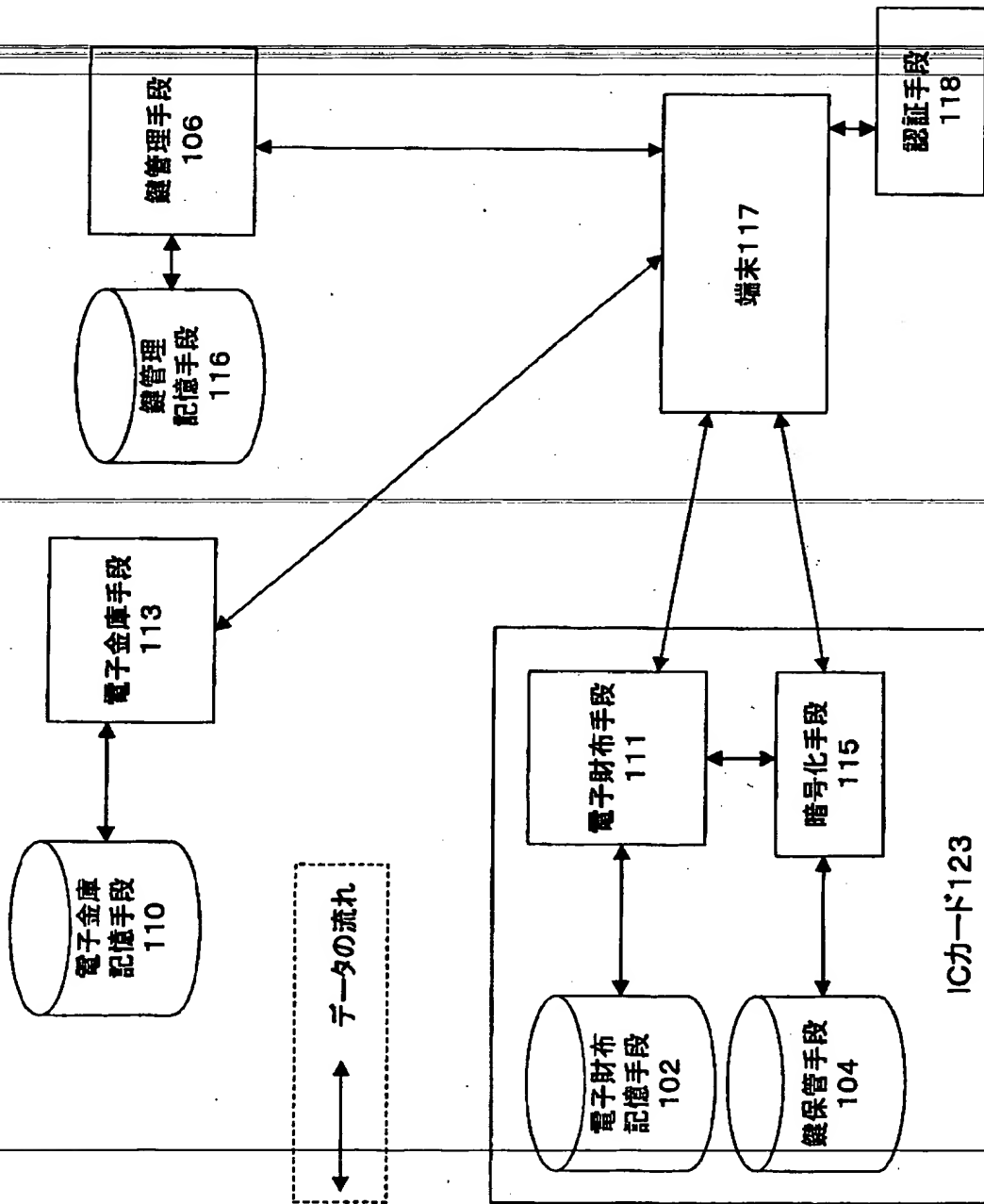
【図 8】



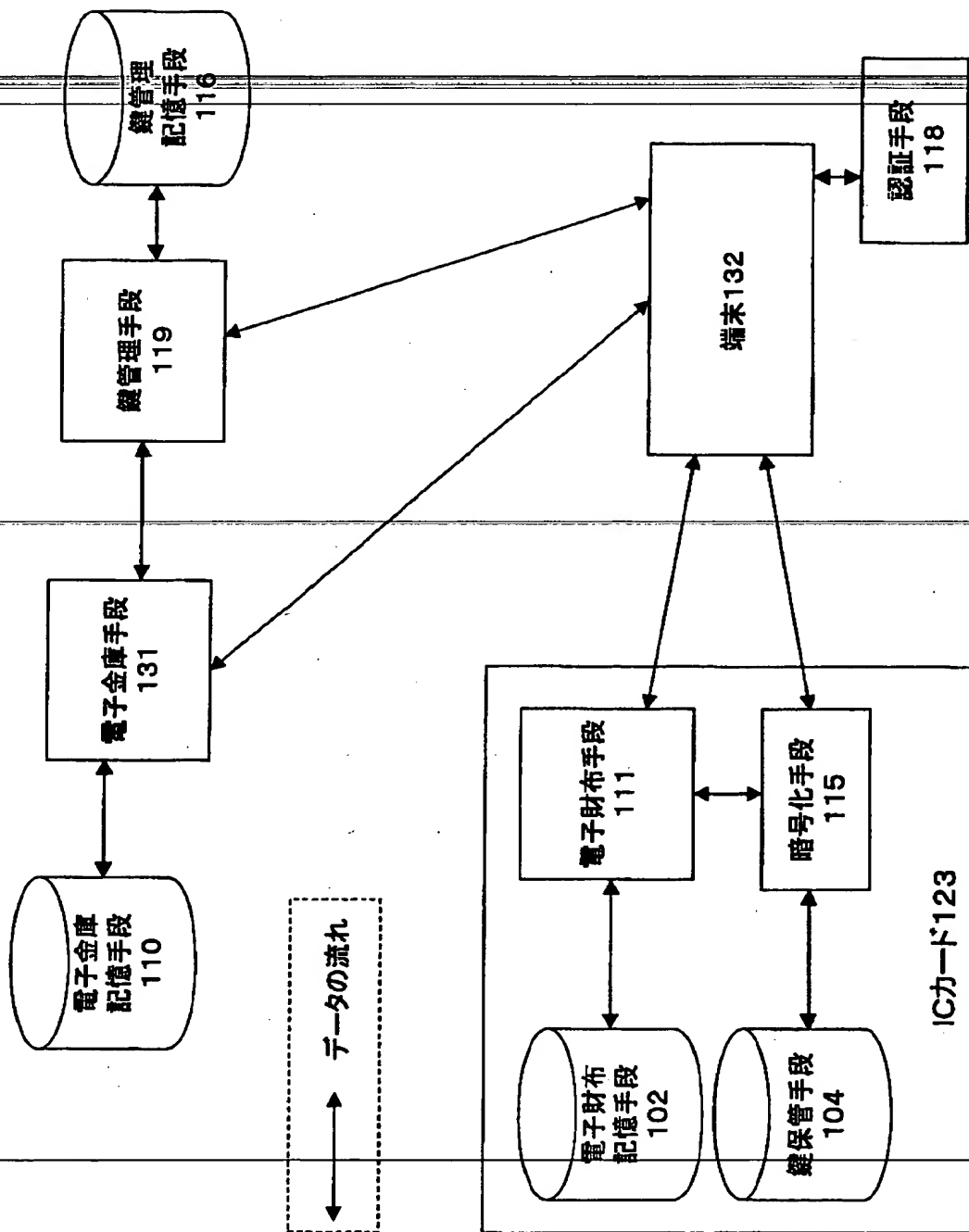
【図 9】



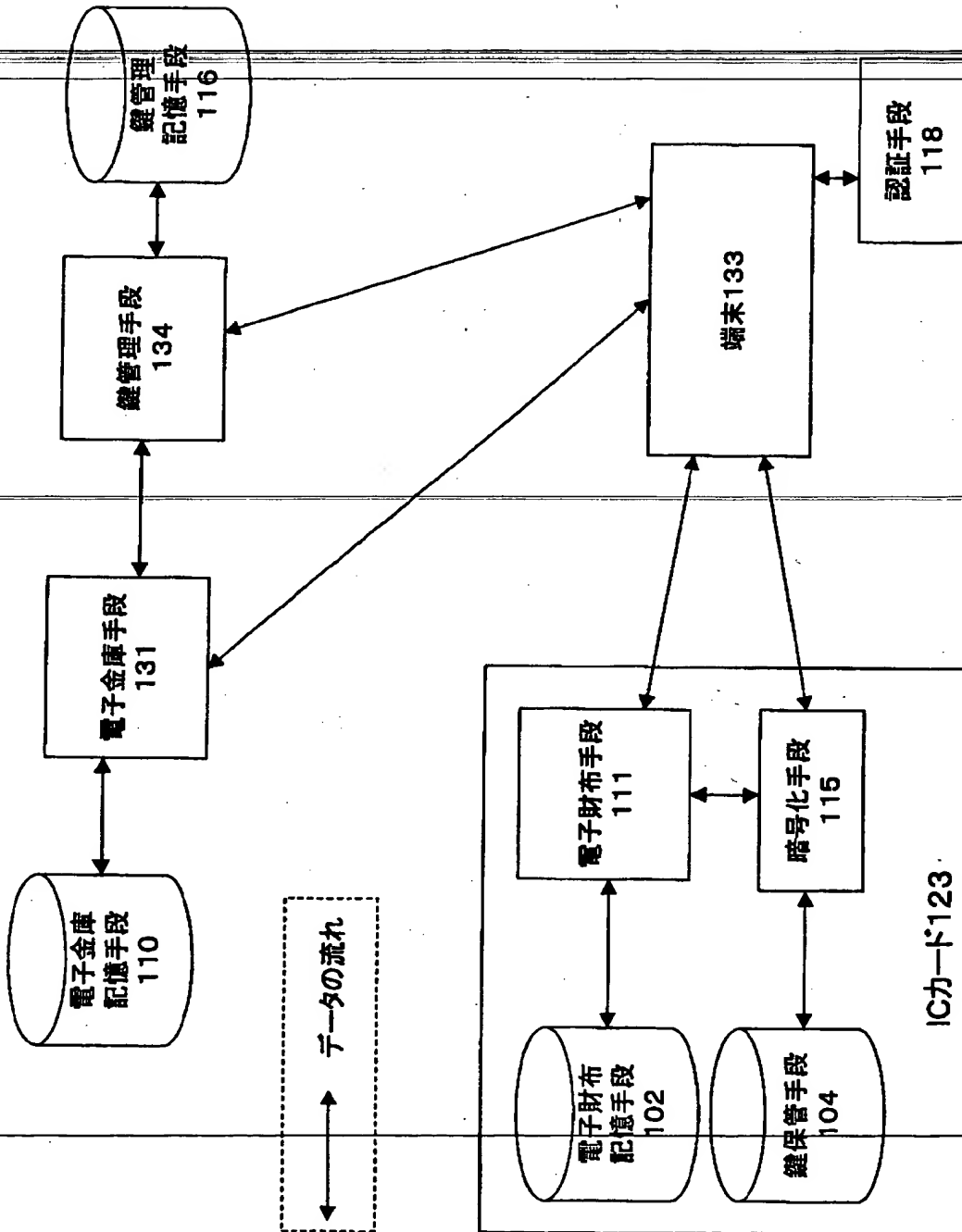
【図 10】



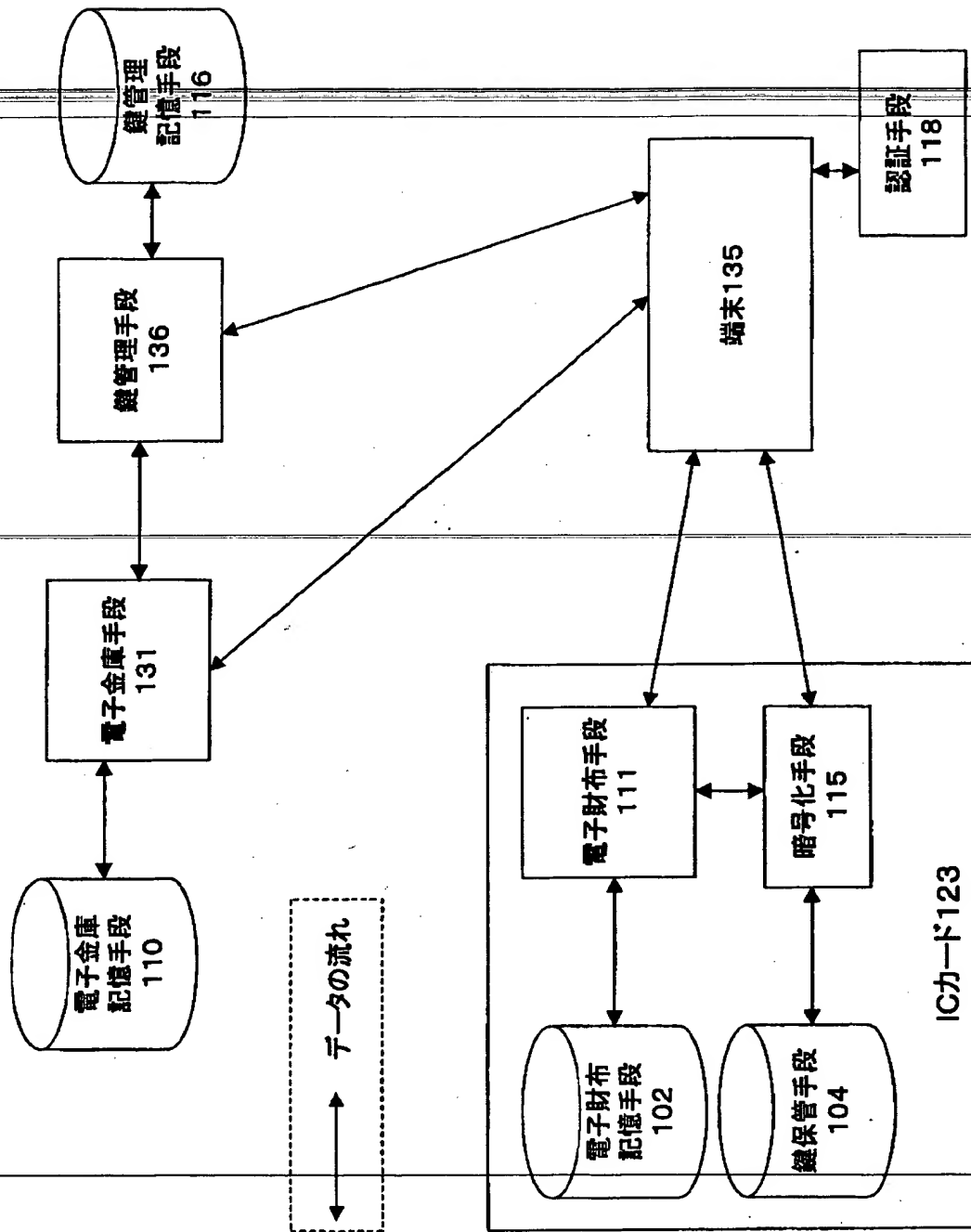
【図 11】



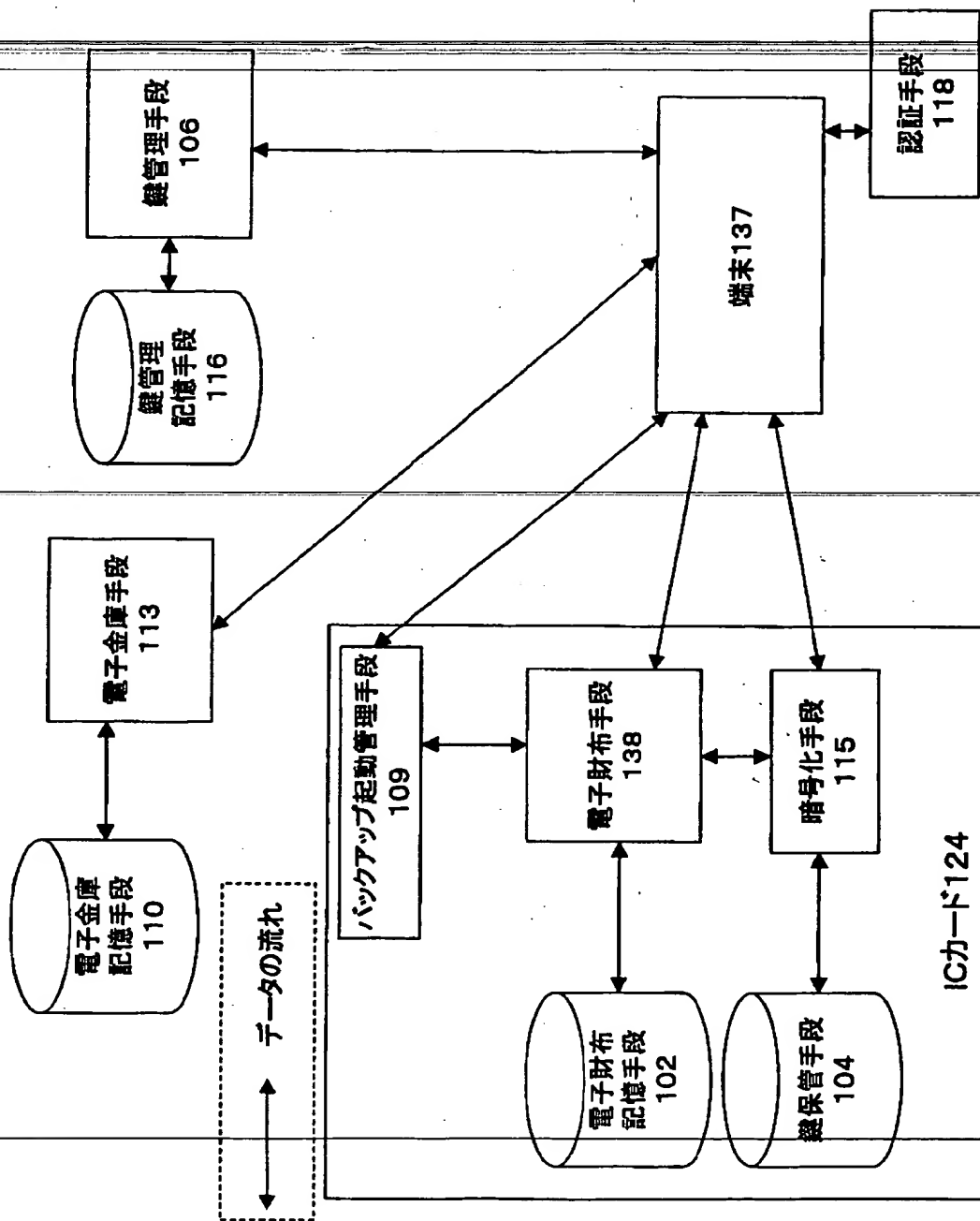
【図 12】



【図 13】



【図 14】



【図 1 5】

情報種別
名前
単価
数
合計金額
場所
有効期間
残金

映画チケット	コンサートチケット
A	C
1600円	4500円
1	2
1600円	9000円
B	D
2000年4月1日～2000年5月31日	2000年4月29日～2000年4月29日
0円	0円

プリペイドカード	映画チケット
E	G
1000円	1600円
1	2
1000円	3200円
F	H
無期限	2000年5月1日～2000年6月30日
800円	0円

【図 16】

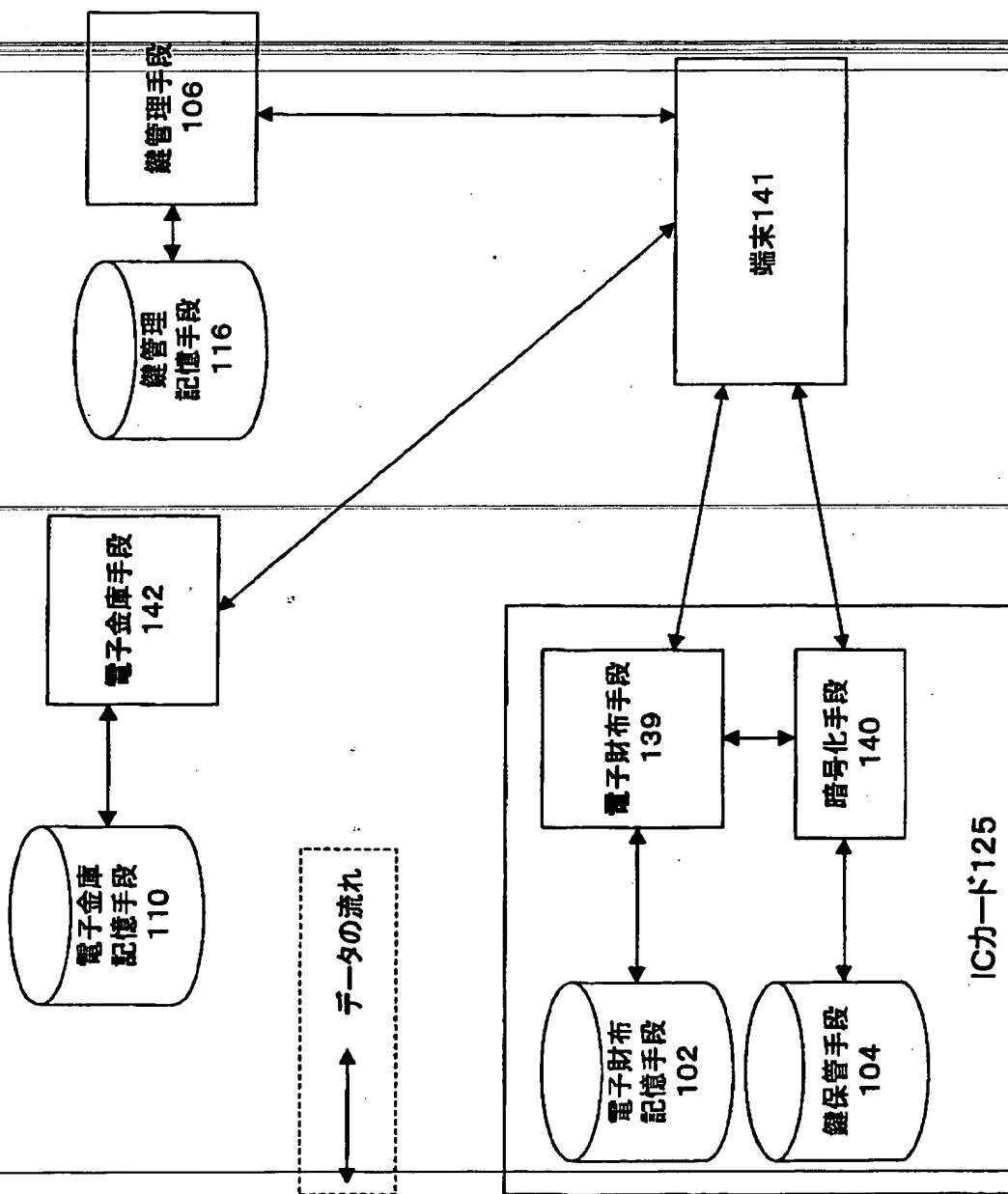
映画チケット	映画チケット
A	G
1600円	1600円
1	2
1600円	3200円
B	H
2000年4月1日～2000年5月31日	2000年5月1日～2000年6月30日
0円	0円

(a)

プリペイドカード	映画チケット
E	G
1000円	1600円
1	2
1000円	3200円
F	H
無期限	2000年5月1日～2000年6月30日
800円	0円

(b)

【図 1 7】



【図 18】

登録電子価値情報204

情報種別	映画チケット
名前	映画タイトル
数	B
場所	劇場名
有効期限	C~D
ダイジェスト302	
暗号化電子価値情報202	
分割復号鍵406	
署名303	

(a)

登録証304

ダイジェスト302	ハッシュ値X2	カウンタ値Y2
-----------	---------	---------

(b)

【書類名】 要約書

【要約】

【課題】 ローカルに存在する電子価値情報の安全性を確保するためのバックアップ手段を提供すること。

【解決手段】 電子財布手段101は電子財布記憶手段102上の電子価値情報を端末100を介して電子金庫手段103に送り、電子金庫手段103は電子価値情報に対する登録証を生成し、電子金庫記憶手段110上に前記電子価値情報と前記登録証を組として保管し、前記登録証を端末100を介して電子財布手段101に返し、電子財布手段101は前記登録証を電子財布記憶手段上に保管する。電子財布手段101は前記登録証を端末100を介して電子金庫手段103に提示することによって、前記登録証に対応する電子価値情報を取得することが可能であり、これによって電子価値情報のバックアップと復元を実現され、電子価値情報の安全性が得られる。

【選択図】 図1

THIS PAGE BLANK (USPTO)